Vol.16No.2(2025):16-43
DOI:https://doi.org/10.61841/turcomat.v16i2.15252

Security and Privacy Challenges in IOT: A Global Perspective

Muhammad Shabbir[1], Mehfooz Ali[2], Mudassir Iftikhar[3]

1. Department of Computer Science, Sindh Madressatul Islam University, Pakistan
Email: m.shabbir1047@gmail.com

2. Department of Computer Science, Sindh Madressatul Islam University, Pakistan
Email: mehfooz.connect@gmail.com

3. Department of Computer Science, Sindh Madressatul Islam University, Pakistan
Email: kb41495@gmail.com

Abstract:
The fast development of the Internet of Things (IoT) has delivered various open doors and advantages across different businesses. Nevertheless, this interconnected biological system of gadgets likewise presents critical security and protection moves that should be tended to on a worldwide scale. This paper looks at the security and protection challenges looked at by IoT frameworks according to a worldwide point of view. Security chances are one more huge worry in the IoT scene. The assortment, stockpiling, and handling of individual information by IoT gadgets bring up issues about individual security privileges. Unapproved admittance to this information can bring about private profiling, reconnaissance, and abuse. Executing security-saving systems like information anonymization, encryption, and client-driven control is fundamental to protecting security in IoT conditions. Administrative systems and guidelines likewise assume a critical part in tending to IoT security and protection challenges. Guidelines like the Overall Information Assurance Guideline (GDPR) in the European Association assist with implementing information security measures and defending client privileges. Be that as it may, variations in guidelines across locales can introduce difficulties for worldwide IoT arrangements. Fitting guidelines and structures can advance consistency and work with worldwide participation. The paper likewise investigates the capability of arising advances in upgrading IoT security and protection. Advancements, for example, block chain, edge registering, and united learning offer promising arrangements. Block chain's decentralized and alter safe nature can give secure information stockpiling and exchange the executives. Edge registering decreases dormancy and information openness by handling information nearer to the source. Combined learning empowers cooperative model preparation while protecting information security. Coordinating these innovations into IoT frameworks can add to a safer and protection-mindful worldwide IoT biological system.

Keywords: *Internet of Things (IoT), IoT Security, Privacy Challenges, Data Protection, Cybersecurity, Encryption, Block chain in IoT, Edge Computing, Regulatory Compliance (GDPR), Federated Learning*

Introduction:

The multiplication of Internet of Things (IoT) gadgets has changed the manner in which we cooperate with the actual world, offering uncommon availability and [1]comfort. Nonetheless, this fast development of IoT has likewise delivered huge security and protection moves that should be tended to on a worldwide scale. The interconnected idea of IoT gadgets joined with the immense measure of information they produce, makes a mind-boggling and dynamic security scene. Also, the assortment and handling of touchy client data raise concerns in regard to security and information assurance. This exploration paper means to investigate the security and protection challenges in IoT according to a worldwide point of view, examining the ramifications and proposing likely arrangements.

The worldwide point of view is urgent while looking at security and protection provokes in IoT because of the interconnected idea of IoT frameworks and the borderless idea of the web. Dangers and weaknesses in a single region of the planet might possibly influence gadgets and organizations on a worldwide scale. Furthermore, contrasting administrative structures and social standards around security add layers of intricacy to tending to these difficulties. Understanding the worldwide scene of IoT security and protection issues is fundamental for creating successful systems and structures to guarantee secure and protection saving IoT arrangements around the world.

This exploration paper will dig into different parts of safety and protection challenges in IoT, including gadget weaknesses, information breaks, confirmation systems, and encryption conventions. It will investigate the effect of these difficulties on clients, associations, and society all in all. Besides, it will look at existing security and protection structures, guidelines, and guidelines in various locales to recognize holes and regions for development.

1.Literature Review:

The fast development of the Internet of Things (IoT) has presented a plenty of safety and security challenges that require [2]extensive investigation and arrangements. In this writing survey, we investigate existing exploration and academic works [3]that shed light on the security and protection challenges in IoT according to a worldwide viewpoint[4]. Various examinations have recognized the security weaknesses present in IoT frameworks[5]. Assault vectors, for example, unapproved access, information altering, and gadget commandeering present critical dangers to the uprightness and accessibility of IoT gadgets and organizations. Analysts have proposed different[6] security components like secure bootstrapping, gadget validation, and interruption recognition frameworks to alleviate these difficulties[7]. The assortment and handling of monstrous measures of individual information by IoT gadgets raise worries about client security. Studies[8] have featured the dangers related with unapproved information divulgence, profiling, and area following. Security safeguarding procedures, for example, information anonymization, secure information sharing conventions,[9] and differential security have been proposed to safeguard client protection while empowering the usefulness of IoT applications[10]. The worldwide viewpoint of IoT security and protection challenges requires a comprehension of administrative[11] systems and principles across various districts. The European Association's Overall Information Insurance Guideline (GDPR) has arisen as a noticeable structure, underlining the [12]privileges of people and information security. Different areas, like the US and Asia-Pacific,

have additionally presented guidelines tending to IoT security and protection[13]. Relative investigations breaking down the qualities and impediments of these structures give significant bits of knowledge to worldwide IoT organizations[14]. The 5g is also provide the features of future IOT. It's open the new challenges[15] on architecture of IOT p2p communication of IOT devices[16]. Guaranteeing secure[17] correspondence between IoT gadgets is pivotal for forestalling unapproved access and information breaks. The writing talks about different encryption and confirmation [18]conventions, for example, Transport Layer Security (TLS), Lightweight cryptography, and Public Key Foundation (PKI). Assessing the qualities and shortcomings of these conventions with regards to worldwide IoT networks helps in recognizing

regions for development[19].

REFRENCES	TITLES	WORKING AND LIMITATION
[20]	The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws	overview of the security, ethical, and privacy challenges faced by the common users
[21]	Security and privacy challenges in IOT	This paper presents an overview of IoT by summarizing its Evolution, Definition, 5-layered architecture, Technologies and IoT Applications
[22]	IOT security and privacy issues	Discuss the iot security and privacy issues
[23]	IoT Privacy and Security: Challenges and Solutions	background of IoT systems and security measures
[24]	Security and Privacy in IoT: A Survey	IoT systems are health care, building smart city with advance construction management system
[25]	Internet of Things – New security and privacy challenges	Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy
[26]	Security and Privacy for Cloud-Based IoT: Challenges	introduce the architecture and unique security and privacy requirements for the next generation mobile technologies on cloud-based IoT
[27]	Privacy and Security Challenges and Solutions in IOT: A review	need for a clear understanding of the issues at hand and how they can be solved
[28]	Privacy and Security Challenges in Internet of Things	discuss security and privacy challenges in IoT scenarios and applications with special emphasis on resource-constrained environments' security objectives and privacy requirement.
[29]	Privacy Challenges and Their Solutions in IoT	identifies various privacy challenges in IoT, and their respective solutions presented by several researches over the time
[30]	IoT Privacy and Security Challenges for Smart Home Environments	financial and human resources available to implement security and privacy vary greatly between application domains

To proactively address security challenges, specialists have proposed danger knowledge structures and discovery systems for IoT. These systems influence AI calculations, peculiarity identification

methods, and conduct examinations to distinguish and relieve security dangers progressively. Worldwide danger insight sharing stages add to an aggregate safeguard approach against worldwide IoT security dangers[31]. Progressions in arising advancements, for example, block chain, edge registering, and united learning, offer expected answers for upgrade security and protection in IoT. Block chain-based arrangements give alter safe information stockpiling and secure exchange the executives. Edge registering empowers limited information handling, [32]decreasing the weakness.

Table 1: Previous Working Table

2. Problem Statement and Discussion:

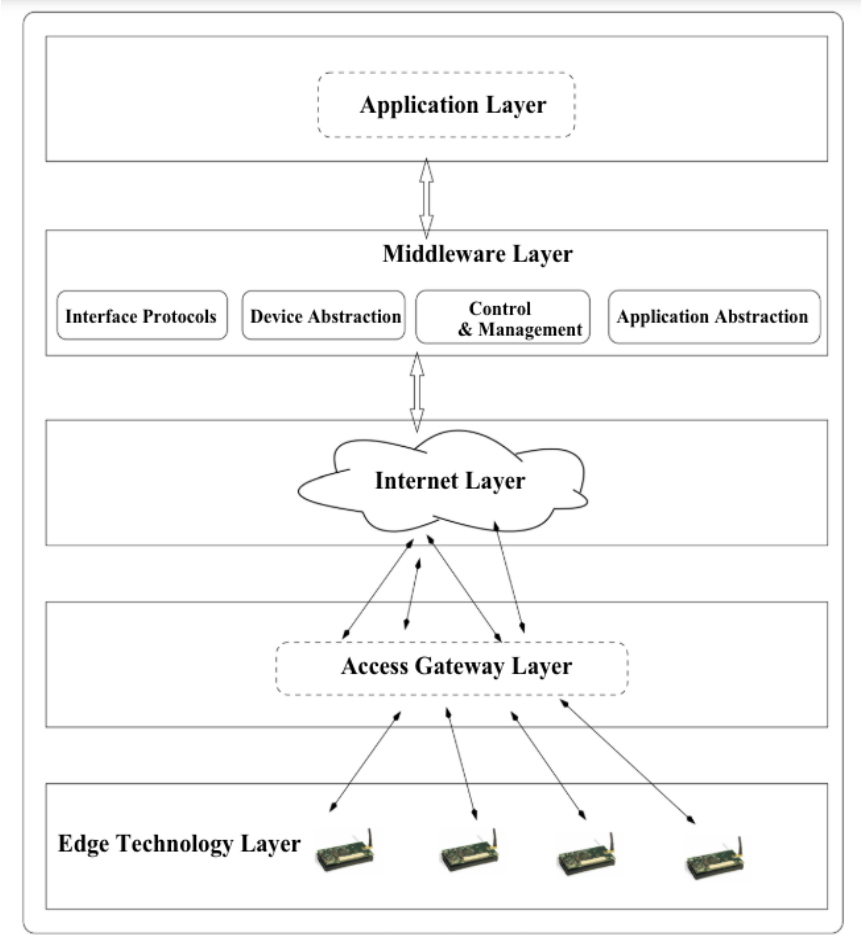

Figure 1 Security Layers [32]

In The Above Figure 1 The use of man-made intelligence and ML(Middle Layer) calculations in IoT security empowers progressed security checking capacities[33]. By dissecting enormous volumes of information continuously, these calculations can [34]distinguish examples, irregularities, and potential security breaks. The robotization of safety strategies through simulated intelligence controlled frameworks works on the productivity and viability of safety tasks, taking into consideration proactive danger identification and reaction.[35]

2.1 Danger Identification in Middle Layers:
Computer based intelligence and Middle Layers calculations offer the upside[36] of proactive danger recognition in IoT frameworks. Not at all like customary safety efforts that depend on known examples or marks, [37]artificial intelligence and Middle Layers procedures can adjust to arising dangers and distinguish beforehand inconspicuous assault vectors. By persistently gaining from authentic information, these calculations can anticipate and moderate potential security gambles before they emerge, lessening the window of weakness for IoT gadgets and organizations[38].2.2 Utilizing Inconsistency Identification in Middle Layer Security
Oddity identification assumes a urgent part in IoT security, and simulated intelligence and ML calculations succeed around here. [39]By laying out examples of typical way of behaving, these calculations can rapidly distinguish deviations or irregularities that might show a security break. Whether it is strange gadget conduct,[40] uncommon organization traffic, or dubious client collaborations, simulated intelligence and ML calculations give extensive insurance against a large number of dangers by distinguishing and making aware of potential security episodes[41].

2.3 Tending to Pre-dispositions and Moral Examinations In Middle Layer
While computer based intelligence and ML calculations offer critical advantages for IoT security, tending to possible inclinations and moral implications[42] is fundamental. Predispositions in preparing information or calculations can bring about oppressive or unreasonable results, compromising [43]protection and security. To guarantee capable and moral use, rules ought to be laid out, advancing straightforwardness, responsibility, and the assurance of client protection and freedoms in the use of simulated intelligence and ML calculations for IoT security[44].

2.4 Powerful Information Assortment and Investigation
The adequacy of man-made intelligence and ML calculations depends on the quality and amount of information they are prepared on. With regards to IoT security, hearty [45]information assortment and investigation rehearses are vital. Secure information the executives, including encryption, secure capacity, and information anonymization, ought to be carried out to safeguard the protection and secrecy[46] of the information gathered from IoT gadgets. By guaranteeing the respectability and dependability of information, the exactness and adequacy of simulated intelligence and ML calculations can be augmented[47].

2.5 Innovative work for Cloud IoT Security

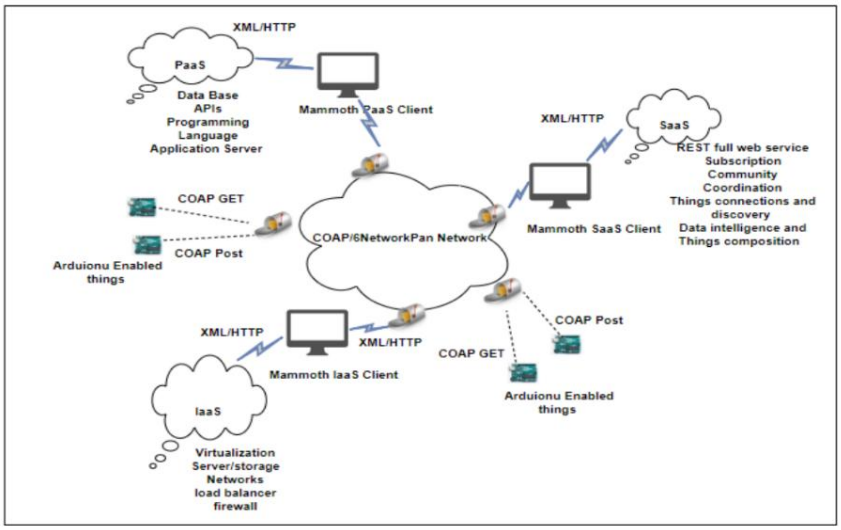

Figure 1 Cloud Security [38]

In The Above Figure 2 To additional improve the capacities of simulated intelligence and CS in IoT security, constant innovative work are important.[48] Headways in profound learning calculations explicitly customized to the one of a kind prerequisites and difficulties of IoT frameworks are significant. This incorporates tending to the restrictions of current calculations, for example, their reliance on unambiguous information [49]models and their weakness to ill-disposed assaults. Continuous development and refinement of man-made intelligence and CS strategies will add to the advancement of IoT security and empower more modern and hearty insurance instruments[50].

By utilizing arising advances, for example, simulated intelligence and CS, the security of IoT frameworks can be fundamentally upgraded. These innovations give [51]progressed observing, proactive danger recognition, oddity identification, and further developed information investigation abilities. In any case, it is vital to move toward their execution morally and capably, tending to predispositions and protection concerns. Progressing innovative work will additionally[52] fortify the capability of computer based intelligence and CS in IoT security, guaranteeing the proceeded with assurance of IoT biological systems in an undeniably associated world[53].

2.6 Discontinuity and the Test of Laying out Steady Security Practices

The shortfall of normalized safety efforts and guidelines in the IoT scene presents huge difficulties to accomplishing worldwide security. The IoT biological system includes many gadgets,[54] conventions, and stages created by various associations and producers, frequently without a brought together security procedure. This [55]discontinuity makes troubles in laying out predictable security rehearses across IoT gadgets, leaving them defenseless against different assaults[56].

2.7 Tending to Discontinuity with a Worldwide Administrative Structure

To defeat the test of fracture and guarantee the security of IoT gadgets, a worldwide administrative system is fundamental. This structure would lay out least security necessities and guidelines that IoT gadgets thought with comply to across borders.[57] As of now, drives like the Online protection Improvement Act in the US and the Network safety Act in the European Association have made strides towards this objective. In any case, more prominent cooperation among partners is important to foster far reaching worldwide norms that can really address security worries on a [58]worldwide scale.

2.8 Reinforcing Security through Cooperative Endeavors

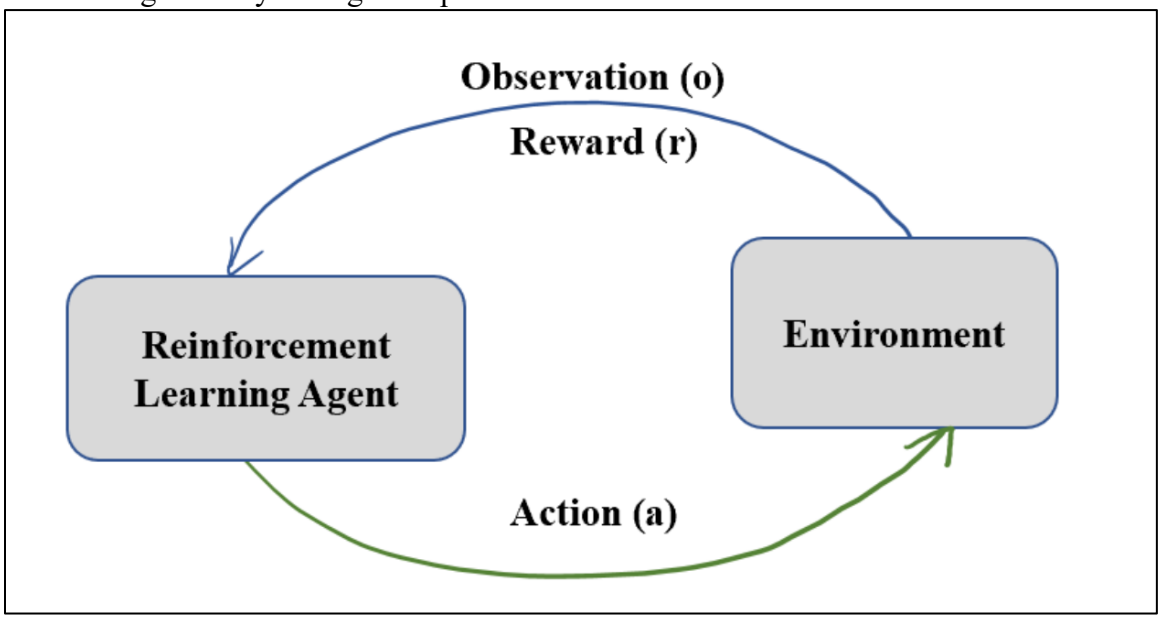

Figure 2 Reinforcement Security [59]

In The Above Figure 3 The Reinforcement Security And The The rising number of dangers and weaknesses focusing on IoT gadgets requires worldwide joint effort to actually alleviate gambles. With the [60]interconnectedness of gadgets, programmers have various section focuses to take advantage of. Normal weaknesses, including insufficient information encryption, unstable correspondence channels, and frail validation instruments, present critical dangers to the security of IoT frameworks.[61] To counter these dangers, legislatures, industry partners, and online protection specialists should cooperate to recognize weaknesses, take on composed weakness the executives rehearses, advance mindful revelation, and offer danger [62]knowledge. Cooperative endeavors, like the IoT Security Stage by the Worldwide Digital Union, give useful direction and devices to carrying out hearty safety efforts.

2.9 Safeguarding Client Protection in IoT Frameworks

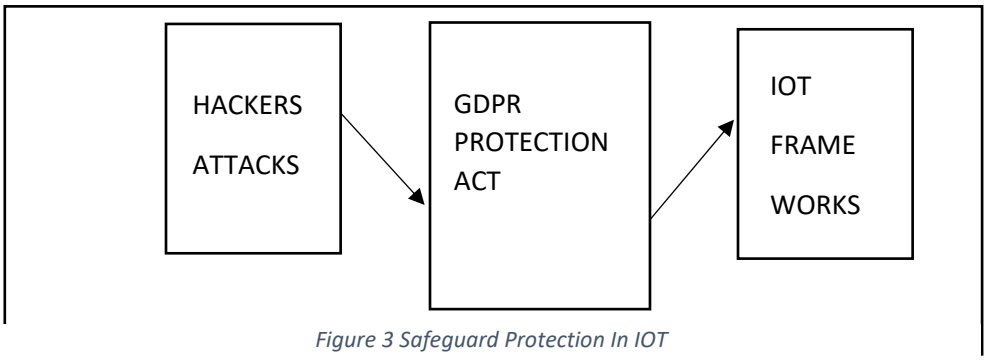

Figure 3 Safeguard Protection In IOT

In The Above Figure 4 The insurance of client protection is a vital part of IoT security that requires worldwide consideration. IoT gadgets frequently gather and cycle immense measures[63] of information without express client assent or information, raising worries about information [64]possession, assent, and straightforwardness. Finding some kind of harmony between the advantages of information assortment and the security of people's protection freedoms is fundamental. Severe information security guidelines, protection by-plan standards, and enabling clients with command over their information are key stages in tending to these [65]difficulties. Guidelines like the Overall Information Security Guideline (GDPR) in the European Association and the California Buyer Protection Act (CCPA) in the US have reinforced information insurance regulations, however fitting protection guidelines across countries and locales stays a basic goal[66].

2.10 Cultivating Cross-Line Coordinated effort for IoT Security

As IoT gadgets rise above public limits, cross-line joint effort becomes imperative in tending to protection and security issues. Given the worldwide idea of digital dangers, a planned methodology is important to battle them really. Worldwide associations, for [67]example, the Web Designing Team (IETF) and the Global Telecom Association (ITU) assume a vital part in working with cooperation and creating worldwide norms. Public-private organizations are instrumental in sharing information, [68]building limit, and thinking up joint methodologies to handle IoT security and protection issues. The Worldwide Discussion on Digital Mastery (GFCE) embodies a global stage that advances collaboration and coordination among different partners[69].

2.11 Saddling Arising Innovations for Upgraded IoT Security

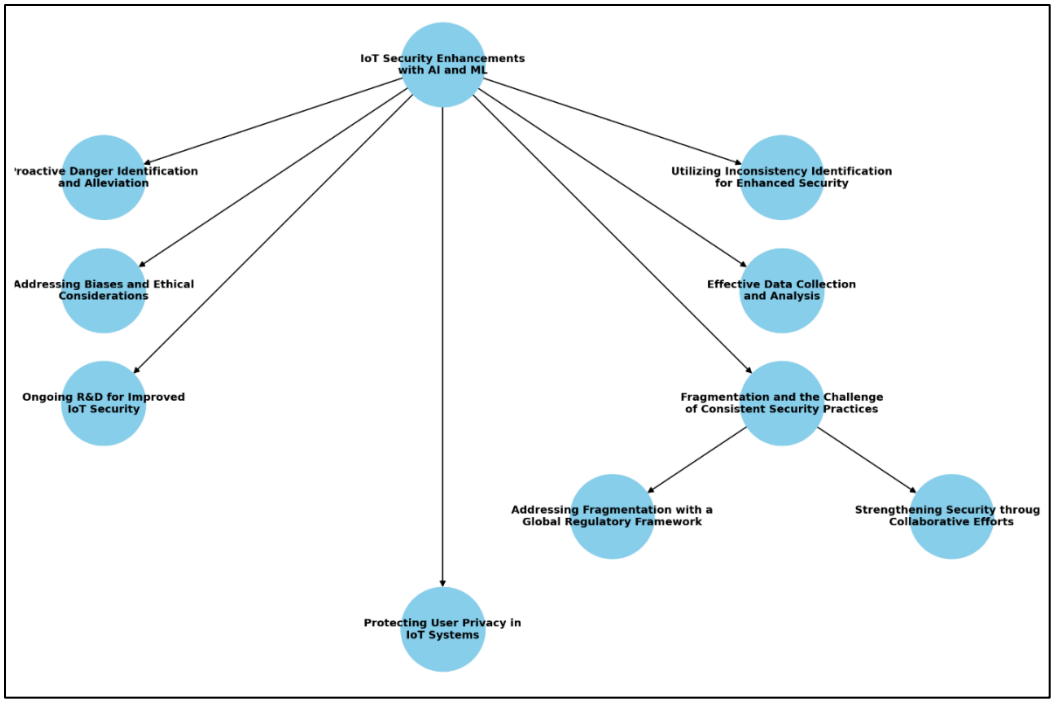

Figure 4 IOT Security In Ai and ML [60]

In The Above Figure 5 identification of [70]peculiarities and potential security dangers. They can mechanize security systems, distinguish dubious way of behaving, and work on the proficiency of reaction instruments. Notwithstanding, it is significant to address expected inclinations and moral ramifications related with these innovations. Laying out moral rules, guaranteeing responsibility,[71] and advancing straightforwardness in the utilization of man-made intelligence and ML in IoT security are fundamental for building trust and protecting client interests.[72]

2.12 Significance of Worldwide Viewpoint:
The interconnected idea of IoT gadgets and organizations rises above geological limits, underlining the requirement for a worldwide viewpoint while tending to security and protection challenges. The exploration [73]discoveries highlight that dangers and weaknesses recognized in one locale can significantly affect IoT frameworks around the world. In this manner,[74] cooperative endeavors among partners from different nations are essential for sharing accepted procedures, organizing reaction components, and blending security and protection norms.

2.13 Tending to Gadget Weaknesses:
The writing audit uncovers that IoT gadgets frequently show weaknesses, making them appealing focuses for pernicious entertainers. To moderate these difficulties,[75] producers ought to take on secure plan standards, including powerful confirmation systems, firmware respectability checks, and secure programming update instruments. Furthermore, making a worldwide [76]storehouse of gadget weaknesses and organizing weakness exposure cycles can work with convenient fixing and decrease the gamble of double-dealing.

2.14 Improving Information Security and Protection:
Safeguarding the protection of client information is of fundamental significance in IoT organizations. Encryption procedures, like start to finish encryption and homomorphic encryption[77], can defend information during transmission and [78]capacity. Furthermore, carrying out security by-plan standards, like information minimization and client driven control, can engage people to have more noteworthy command over their information. Worldwide administrative structures, similar to the GDPR, can act as a model for fitting security guidelines and cultivating client trust in IoT frameworks.

Cooperation for Danger Knowledge:
The conversation accentuates the worth of worldwide joint effort in sharing danger knowledge to distinguish and answer arising IoT security dangers. Laying out stages and systems for sharing danger data can work with ongoing danger investigation and [79]empower associations to foster compelling relief procedures. Such joint effort can encourage a proactive security act, upgrading the general versatility of IoT frameworks on a worldwide scale.

2.15 Arising Advancements for Security:
The conversation features the capability of arising advancements, for example, blockchain, edge figuring, and combined learning, intending to IoT security and protection challenges. Blockchain can give alter safe and decentralized information [80]capacity, guaranteeing the honesty and

straightforwardness of IoT exchanges. Edge figuring lessens information openness and dormancy by handling information locally, limiting the assault surface. United learning permits cooperative model preparation without uncovering touchy client information, protecting security [81].

2.16 Worldwide IoT system Application:

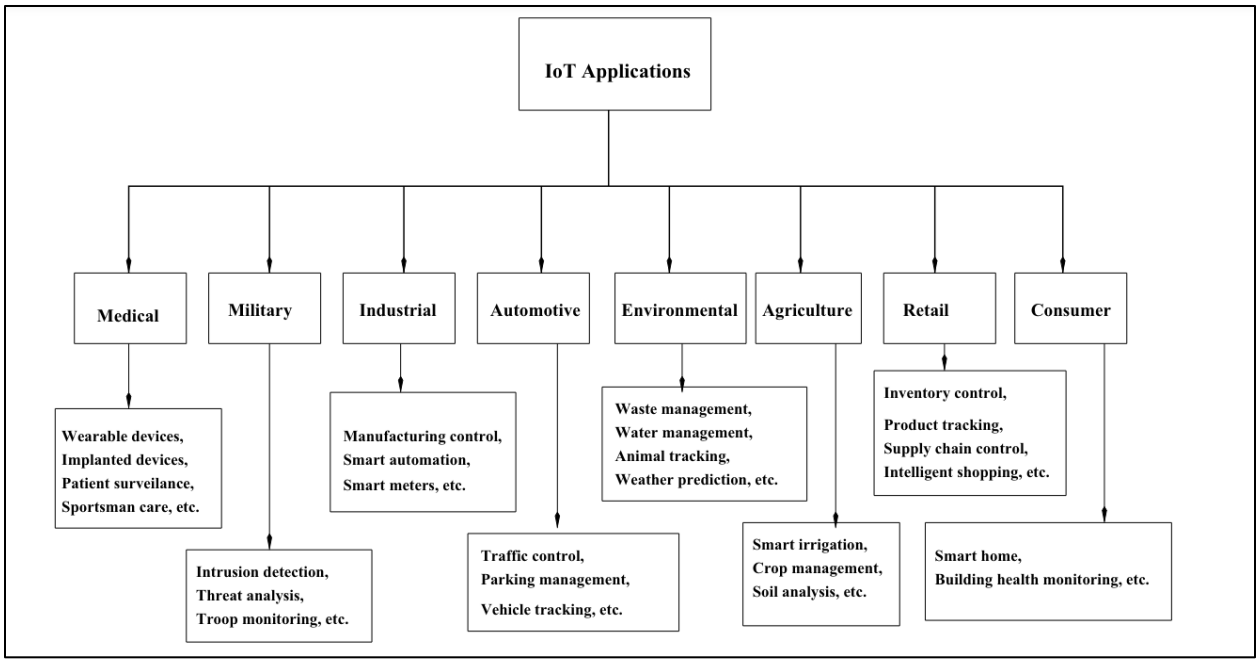

Figure 5 Application Of IOT Security [73]

In The Above Figure 6 In view of the examination of the writing survey, the conversation segment presents a few proposals to encourage a protected worldwide IoT environment.[82] These incorporate the foundation of worldwide coordinated effort structures to share best practices and danger knowledge, the [83]improvement of normalized security and protection rules for IoT gadget producers, and the advancement of client schooling and mindfulness about security and protection chances. Also, it stresses the requirement for nonstop examination and advancement to stay up with advancing security dangers and the improvement of secure-by-plan IoT structures[84].

2.17 Worldwide Coordinated effort:

Given the worldwide idea of IoT, tending to security and protection challenges requires global coordinated effort. Digital dangers rise above geological limits, and powerful arrangements require the aggregate endeavors of states, associations, and [85]security networks around the world. Sharing danger knowledge, planning episode reaction, and orchestrating administrative systems are significant stages toward building an aggregate protection against IoT-related gambles [86].

Coordinated effort between industry partners is likewise fundamental. Gadget producers, network suppliers, and programming engineers need to team up to lay out security best practices, direct security reviews, and advance the reception of secure innovations. Data sharing stages and

associations can work with the spread of information and [87]assist associations with remaining informed about arising dangers and countermeasures.

2.18 Military Application and Measures in IOT:

Military structures assume a fundamental part in tending to security and protection challenges in IoT. States and administrative bodies have an obligation to lay out regulations and guidelines that [88]safeguard people's protection freedoms and guarantee the security of IoT frameworks. The Overall Information Assurance Guideline (GDPR) in the European Association, for instance, has presented severe prerequisites for information security and protection[89].

Harmonization of guidelines across various areas is urgent to keep away from errors that might block worldwide IoT arrangements. Coordinated effort between Military administrative bodies, industry affiliations, and [90]normalization associations is expected to foster reliable systems that address security and protection worries while encouraging development.

2.19 Block chain Innovations:

The combination of arising advances can altogether add to upgrading the security and protection of IoT frameworks. Block chain innovation, with its decentralized and alter safe nature, can give secure information stockpiling, character[90].

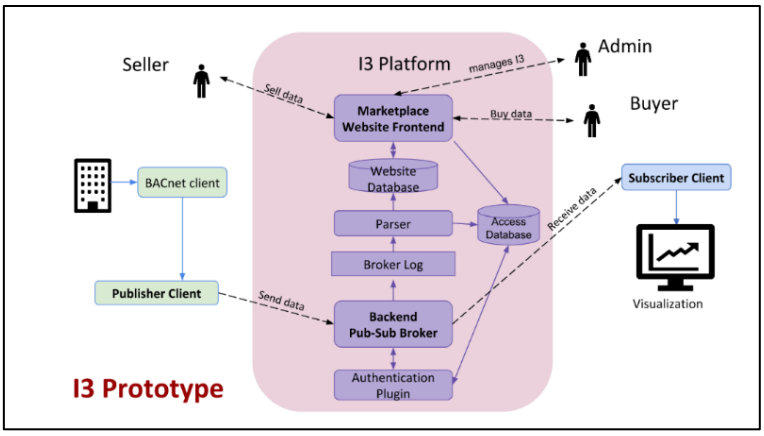

Figure 6 E-commerce Through IOT [80]

2.20 IOT Marketplace:

In The Above Figure 7 It is estimated 1.5 billion internet-enable pcs and 1 billion internet-enable mobile phones. In future the will be around 50 billion device connected to internet [91]

2.21 Lacking Safety efforts in IoT Gadgets

With the multiplication of Web of Things (IoT) gadgets, there has been a critical expansion in the quantity of dangers and weaknesses focusing on these gadgets[92]. One of the essential purposes behind this is the lacking safety efforts carried out in IoT gadgets. Numerous IoT gadgets need powerful security highlights, making them helpless against assaults[93].

2.22 Absence of Information Encryption

Information encryption is a basic part of safety, particularly with regards to safeguarding delicate data sent over IoT organizations. Notwithstanding, various IoT gadgets neglect to integrate appropriate [94]information encryption systems. This leaves the information powerless against

capture and unapproved access. Without encryption, programmers can undoubtedly capture and control the information, compromising the respectability and privacy of the data[95].

2.23 Fail Validation Instruments

Confirmation is essential for guaranteeing that main approved people or gadgets can get to IoT organizations and gadgets.[96] Tragically, numerous IoT gadgets have frail verification instruments or even need them altogether. This makes it simpler for aggressors to acquire unapproved admittance to the gadgets and take [97]advantage of their functionalities. Frail or default passwords, absence of multifaceted verification, and deficient access controls all add to the weakness of IoT gadgets.

2.24 Vulnerabilities and Challenges in IOT Channels:

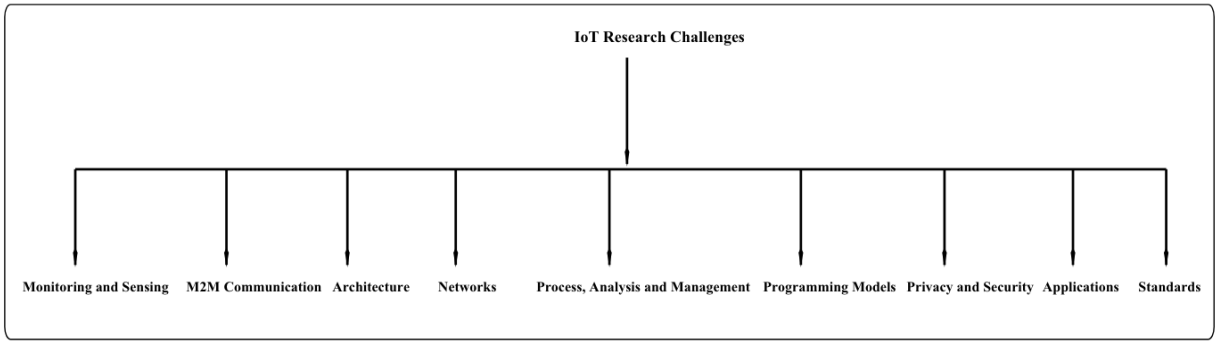

Figure 7 challenges in IOT Channels [87]

IoT gadgets depend on correspondence channels, like Wi-Fi, Bluetooth, or cell organizations, to communicate information and interface with different gadgets or frameworks. Notwithstanding, these correspondence channels frequently have weaknesses that can be taken advantage of by assailants. Shaky conventions, frail encryption, or absence of appropriate [98]organization division can open IoT gadgets to different security gambles. Aggressors can block or control the information being sent, prompting unapproved access or noxious activities.

2.25 Interconnectedness and Intensification of Dangers

The interconnected idea of IoT gadgets represents extra difficulties and enhances the dangers related with security weaknesses. Generally speaking, a solitary compromised IoT gadget can act as a door for aggressors to penetrate a whole organization[99] or framework. This interconnectedness permits aggressors to use compromised gadgets as takeoff platforms for additional assaults, possibly compromising delicate information or even basic framework[100].

2.26 Taking advantage of a Solitary Compromised Gadget

A solitary compromised IoT gadget can have expansive outcomes. Assailants can oversee the compromised gadget and use it as a venturing stone to get to different gadgets or frameworks inside a similar organization. This sidelong development expands the degree and effect of the assault. Moreover, compromised gadgets can likewise be utilized to send off conveyed disavowal of-administration (DDoS) [101]assaults, where countless compromised gadgets are facilitated to overpower an objective framework or organization.

2.27 Penetration of Organizations and Frameworks

The interconnectedness of IoT gadgets makes organizations and frameworks more powerless against invasion. Aggressors can take advantage of weaknesses in a single gadget to get close enough to the whole organization or framework[102]. When inside, they can move horizontally, compromising different gadgets, getting to delicate [103]information, or in any event, upsetting basic activities. This capacity to penetrate and proliferate inside an organization or framework builds the intricacy of distinguishing and moderating assaults.

2.28 Through Security Systems for IoT

Tending to the rising dangers and weaknesses in IoT requires thorough security systems that envelop various layers of safeguard. Powerful safety efforts should be carried out at the gadget level, secure correspondence channels, weakness the board, and dependable divulgence rehearses[104].

2.29 Gadget Level Safety efforts

Carrying areas of strength for out measures at the gadget level is urgent to shield IoT gadgets from assaults. This incorporates consolidating strong encryption calculations to get information both very still and on the way. Furthermore, gadgets ought to have powerful verification systems, for example, multifaceted confirmation, to guarantee that main approved elements can get to them[105].

2.30 Encryption Calculations and Security In IOT:

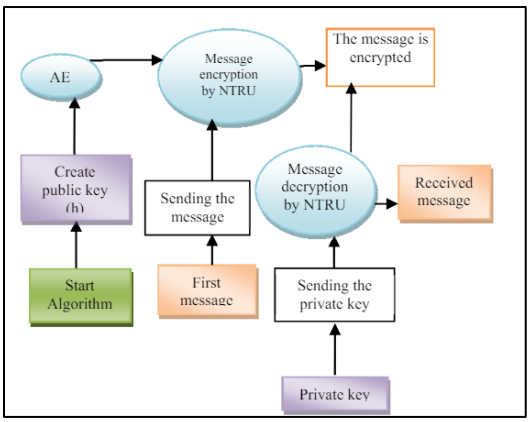

Figure 8 DE in IOT [95]

In The Above Figure 9 Executing solid encryption calculations, like High Level Encryption Standard (AES), guarantees that the information communicated between IoT gadgets and organizations stays secret and carefully designed. Encryption calculations ought to be appropriately carried out and[106]

2.31 Security of Client Protection

In the time of the Web of Things (IoT), where a rising number of gadgets are interconnected and gathering tremendous measures of information, the security of client protection has turned into a basic concern. IoT gadgets frequently assemble touchy data without clients' unequivocal [107]assent or information, raising huge protection challenges. Adjusting the advantages of information assortment for further developed administrations with the security of people's protection privileges is fundamental in tending to these worries.

2.32 Information Assortment and Assent

One of the key security issues in the IoT environment is the assortment of individual information without clients' express assent. IoT gadgets, going from brilliant home gadgets to wearable wellness trackers, consistently gather and cycle a large number of information, including individual and conduct data. This information might incorporate by and by recognizable data (PII), area information, wellbeing information, from there, the sky is the limit. Clients frequently have restricted [108]consciousness of the information being gathered and the way things are being utilized.

To safeguard client security, upholding severe information assurance regulations is urgent. Measures like the Overall Information Security Guideline (GDPR) in the European Association and the California Customer Protection Act (CCPA) in the US mean to give people more noteworthy command over their own information. These guidelines underline the requirement for informed assent, straightforwardness, and the option to quit information assortment rehearses[109].

2.33 Security by-Plan Standards

Security by-plan is a methodology that promoters for protection contemplations to be incorporated into the plan and advancement of IoT frameworks all along. By integrating protection upgrading highlights and systems into IoT gadgets and administrations, the gamble of security breaks can be limited. Protection by-plan standards incorporate information minimization, reason limit, client driven control, and information security[110].

Information minimization includes gathering just the fundamental information to satisfy the expected reason and staying away from unnecessary information assortment. Reason constraint guarantees that gathered information is utilized exclusively for the predefined purposes and not shared or utilized for other inconsequential exercises. Client driven control enables people to have

command over their information, permitting them to get to, make due, and erase their information depending on the situation. Information safety efforts, like encryption and secure stockpiling, are fundamental to shield individual information from unapproved access[111].

3 Future Scope:

The conversation segment centers around dissecting the critical discoveries and ramifications of the exploration directed on security and protection challenges in IoT according to a worldwide viewpoint. It features the meaning of tending to these difficulties and proposes expected methodologies and suggestions which will be come in future[112].

3.1 Significance of Worldwide Viewpoint:

The interconnected idea of IoT gadgets and organizations rises above geological limits, underlining the requirement for a worldwide viewpoint while tending to security and protection challenges. The exploration discoveries highlight that dangers and weaknesses recognized in one locale can significantly affect IoT frameworks around the world. In this manner, cooperative endeavors among partners from different nations are essential for sharing accepted [113]procedures, organizing reaction components, and blending security and protection norms.

3.2 Improving the Gadget Weaknesses:
The writing audit uncovers that IoT gadgets frequently show weaknesses, making them appealing focuses for pernicious entertainers. To moderate these difficulties, producers ought to take on secure plan standards, including powerful confirmation systems, firmware respectability checks, and secure programming update instruments. Furthermore, making a worldwide storehouse of gadget weaknesses and organizing weakness exposure cycles can work with convenient fixing and decrease the gamble of double-dealing[114].

3.3 Improving Information Security and Protection:
Safeguarding the protection of client information is of fundamental significance in IoT organizations. Encryption procedures, like start to finish encryption and homomorphic encryption, can defend information during transmission and capacity. Furthermore, carrying out security by-plan standards, like information minimization and client driven control, can engage people to have more noteworthy command over their information. Worldwide administrative structures, similar to the GDPR, can act as a model for fitting security guidelines and cultivating client trust in IoT frameworks[115].

3.4 Keep Save To IoT frameworks on a worldwide scale:
The conversation accentuates the worth of worldwide joint effort in sharing danger knowledge to distinguish and answer arising IoT security dangers. Laying out stages and systems for sharing danger data can work with ongoing danger investigation and empower associations to foster compelling relief procedures. Such joint effort can encourage a proactive security act, upgrading the general versatility of IoT frameworks on a worldwide scale[116].

3.5 Implement Block chain for Security:
The conversation features the capability of arising advancements, for example, block chain, edge figuring, and combined learning, intending to IoT security and protection challenges. Block chain can give alter safe and decentralized information capacity, guaranteeing the honesty and straightforwardness of IoT exchanges. Edge figuring lessens information openness and dormancy by handling information locally, limiting the assault surface. United learning permits cooperative model preparation without uncovering touchy client information, protecting security[117].

3.6 Proposals for a Safe Worldwide IoT Biological system:
In view of the examination of the writing survey, the conversation segment presents a few proposals to encourage a protected worldwide IoT environment. These incorporate the foundation of worldwide coordinated effort structures to share best practices and danger knowledge, the improvement of normalized security and protection rules for IoT gadget producers, and the advancement of client schooling and mindfulness about security and protection chances. Also, it stresses the requirement for nonstop examination and advancement to stay up with advancing security dangers and the improvement of secure-by-plan IoT structures[118].

Conclusion:
The worldwide point of view on security and protection challenges in IoT uncovers the critical requirement for complete measures to address the weaknesses and dangers related with

interconnected IoT frameworks. This examination paper has inspected the vital discoveries and suggestions from the writing survey, featuring the significance of a worldwide way to deal with handling these difficulties.
The examination has uncovered that IoT gadgets are powerless to weaknesses because of deficient safety efforts during plan and advancement. These weaknesses can prompt unapproved access, information breaks, and noxious control, with potential effects going from individual protection encroachments to disturbances in basic framework. Moreover, the assortment and handling of individual information by IoT gadgets raise worries about security, requiring the execution of protection saving systems to safeguard client freedoms[119].

A cooperative methodology is significant for relieving IoT security dangers on a worldwide scale. Sharing danger insight, organizing episode reaction, and orchestrating administrative structures can assist with laying out an aggregate guard component. Moreover, arising advancements, for example, block chain, edge registering, and unified learning, offer promising answers for upgrade IoT security and protection. Incorporating these[120] innovations can add to a safer and security mindful worldwide IoT environment.

All in all, tending to the security and protection challenges in IoT requires a purposeful exertion from partners around the world. By focusing on gadget security, safeguarding client protection, encouraging worldwide joint effort, and utilizing arising innovations, we can make a stronger and reliable IoT climate. It is fundamental to lay out normalized systems, advance client mindfulness, and empower ceaseless exploration and development to remain in front of developing dangers[121].
By carrying out the proposals and procedures proposed in this examination paper, partners can prepare for a protected and security safeguarding worldwide IoT biological system. This won't just guarantee the security of delicate information yet in addition open the maximum capacity of IoT advances in different areas, cultivating development, proficiency, and worked on personal satisfaction. With a worldwide [122]viewpoint and cooperative endeavors, we can conquer the difficulties and construct a future where IoT frameworks are secure, protection cognizant, and valuable for all.

References

[1] P. Tuwanut and S. Kraijak, “A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends,” in *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, Shanghai, China: Institution of Engineering and Technology, 2015, p. 6 .-6 . doi: 10.1049/cp.2015.0714.
[2] H. A. Abdul-Ghani and D. Konstantas, “A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective,” *J. Sens. Actuator Netw.*, vol. 8, no. 2, p. 22, Apr. 2019, doi: 10.3390/jsan8020022.
[3] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, “A decentralized approach for security and privacy challenges in the Internet of Things,” in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea (South): IEEE, Mar. 2014, pp. 67–72. doi: 10.1109/WF-IoT.2014.6803122.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.
[5] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, 2018.
[6] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet Things*, vol. 14, p. 100129, 2021.
[7] A. B. Pawar and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures," in *2016 international conference on computing, analytics and security trends (CAST)*, IEEE, 2016, pp. 294–299. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7914983/
[8] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
[9] R. Kumar, P. Kumar, and V. Singhal, "A survey: Review of cloud IoT security techniques, issues and challenges," in *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, 2019. Accessed: Mar. 29, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350995
[10] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, 2020.
[11] T. Mazhar *et al.*, "Analysis of IoT security challenges and its solutions using artificial intelligence," *Brain Sci.*, vol. 13, no. 4, p. 683, 2023.
[12] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, Jan. 2021, doi: 10.1109/JIOT.2020.3008906.
[13] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, 2019.
[14] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, 2019.
[15] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, 2017.
[16] S. N. Mohanty *et al.*, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.
[17] R. C. Poonia, "Internet of Things (IoT) security challenges," in *Handbook of e-business security*, Auerbach Publications, 2018, pp. 191–223. Accessed: Mar. 29, 2024. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9780429468254-8/internet-things-iot-security-challenges-ramesh-poonia
[18] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3677.

[19] R. F. Ali, A. Muneer, P. D. D. Dominic, S. M. Taib, and E. A. A. Ghaleb, "Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review," in *Advances in Cyber Security*, vol. 1487, N. Abdullah, S. Manickam, and M. Anbar, Eds., in Communications in Computer and Information Science, vol. 1487. , Singapore: Springer Singapore, 2021, pp. 128–154. doi: 10.1007/978-981-16-8059-5_9.
[20] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet Things*, vol. 15, p. 100420, 2021.
[21] M. S. Virat, S. M. Bindu, B. Aishwarya, B. N. Dhanush, and M. R. Kounte, "Security and privacy challenges in internet of things," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2018, pp. 454–460. Accessed: Jun. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8553919/
[22] A. Assiri and H. Almagwashi, "IoT security and privacy issues," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, IEEE, 2018, pp. 1–5. Accessed: Jun. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8442002/
[23] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, 2020.
[24] P. M. Chanal and M. S. Kakkasageri, "Security and Privacy in IoT: A Survey," *Wirel. Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, Nov. 2020, doi: 10.1007/s11277-020-07649-9.
[25] R. H. Weber, "Internet of Things–New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.
[26] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, 2017.
[27] N. Alhalafi and P. Veeraraghavan, "Privacy and Security Challenges and Solutions in IOT: A review," in *IOP conference series: Earth and environmental science*, IOP Publishing, 2019, p. 012013. Accessed: Jun. 28, 2024. [Online]. Available: https://iopscience.iop.org/article/10.1088/1755-1315/322/1/012013/meta
[28] M. L. Das, "Privacy and Security Challenges in Internet of Things," in *Distributed Computing and Internet Technology*, vol. 8956, R. Natarajan, G. Barua, and M. R. Patra, Eds., in Lecture Notes in Computer Science, vol. 8956. , Cham: Springer International Publishing, 2015, pp. 33–48. doi: 10.1007/978-3-319-14977-6_3.
[29] N. Hasan, A. Chamoli, and M. Alam, "Privacy Challenges and Their Solutions in IoT," in *Internet of Things (IoT)*, M. Alam, K. A. Shakil, and S. Khan, Eds., Cham: Springer International Publishing, 2020, pp. 219–231. doi: 10.1007/978-3-030-37468-6_11.
[30] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.
[31] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, 2018, doi: 10.1016/j.procs.2018.05.140.
[32] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 12–18, Dec. 2018, doi: 10.1109/MWC.2017.1800116.
[33] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: current status, challenges and countermeasures," *Int. J. Inf. Secur. Res. IJISR*, vol. 5, no. 4, pp. 608–616, 2015.

[34] R. H. Weber, "Internet of Things – New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010, doi: 10.1016/j.clsr.2009.11.008.
[35] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *2015 10th international conference for internet technology and secured transactions (ICITST)*, IEEE, 2015, pp. 336–341. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7412116/
[36] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," in *2015 International conference on green computing and internet of things (ICGCIoT)*, Ieee, 2015, pp. 1577–1581. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7380718/
[37] H. Wang, Z. Zhang, and T. Taleb, "Editorial: Special Issue on Security and Privacy of IoT," *World Wide Web*, vol. 21, no. 1, pp. 1–6, Jan. 2018, doi: 10.1007/s11280-017-0490-9.
[38] E. Shaikh, I. Mohiuddin, and A. Manzoor, "Internet of Things (IoT): Security and Privacy Threats," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia: IEEE, May 2019, pp. 1–6. doi: 10.1109/CAIS.2019.8769539.
[39] I. Yaqoob *et al.*, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017, doi: 10.1109/MWC.2017.1600421.
[40] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of things security: challenges and key issues," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, 2021.
[41] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
[42] N. Miloslavskaya and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Clust. Comput.*, vol. 22, no. 1, pp. 103–119, Mar. 2019, doi: 10.1007/s10586-018-2823-6.
[43] P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, "Internet of Things: Applications, security and privacy: A survey," *Mater. Today Proc.*, vol. 34, pp. 752–759, 2021, doi: 10.1016/j.matpr.2020.04.737.
[44] D. Mendez Mena, I. Papapanagiotou, and B. Yang, "Internet of things: Survey on security," *Inf. Secur. J. Glob. Perspect.*, vol. 27, no. 3, pp. 162–182, May 2018, doi: 10.1080/19393555.2018.1458258.
[45] D. M. Mendez, I. Papapanagiotou, and B. Yang, "Internet of Things: Survey on Security and Privacy," 2017, doi: 10.48550/ARXIV.1707.01879.
[46] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*, IEEE, 2015, pp. 180–187. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7405513/
[47] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Dalian, China: IEEE, Oct. 2011, pp. 709–712. doi: 10.1109/iThings/CPSCom.2011.83.
[48] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[49] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd Annual Design Automation Conference*, San Francisco California: ACM, Jun. 2015, pp. 1–6. doi: 10.1145/2744769.2747942.
[50] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, 2020.
[51] H. C. Chen, M. A. A. Faruque, and P. H. Chou, "Security and privacy challenges in IoT-based machine-to-machine collaborative scenarios," in *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*, Pittsburgh Pennsylvania: ACM, Oct. 2016, pp. 1–2. doi: 10.1145/2968456.2974008.
[52] A. Cirne, P. R. Sousa, J. S. Resende, and L. Antunes, "IoT security certifications: Challenges and potential approaches," *Comput. Secur.*, vol. 116, p. 102669, 2022.
[53] Z. Xihua and Dr. S. B. Goyal, "Security and Privacy Challenges using IoT-Blockchain Technology in a Smart City: Critical Analysis," *Int. J. Electr. Electron. Res.*, vol. 10, no. 2, pp. 190–195, Jun. 2022, doi: 10.37391/ijeer.100224.
[54] A. M. Abuagoub, "IoT security evolution: challenges and countermeasures review," *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 3, pp. 342–351, 2019.
[55] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Aalborg, Denmark: IEEE, May 2014, pp. 1–8. doi: 10.1109/PRISMS.2014.6970594.
[56] J. Mohanty, S. Mishra, S. Patra, B. Pati, and C. R. Panigrahi, "IoT Security, Challenges, and Solutions: A Review," in *Progress in Advanced Computing and Intelligent Engineering*, vol. 1199, C. R. Panigrahi, B. Pati, P. Mohapatra, R. Buyya, and K.-C. Li, Eds., in Advances in Intelligent Systems and Computing, vol. 1199. , Singapore: Springer Singapore, 2021, pp. 493–504. doi: 10.1007/978-981-15-6353-9_46.
[57] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks & defenses," in *2017 international conference on Communication Technologies (ComTech)*, IEEE, 2017, pp. 104–110. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8065757/
[58] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia: IEEE, May 2017, pp. 1292–1297. doi: 10.23919/MIPRO.2017.7973622.
[59] A. Uprety and D. B. Rawat, "Reinforcement learning for iot security: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8693–8706, 2020.
[60] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet Things*, vol. 15, p. 100420, Sep. 2021, doi: 10.1016/j.iot.2021.100420.
[61] M. Litoussi, N. Kannouf, K. El Makkaoui, A. Ezzati, and M. Fartitchou, "IoT security: challenges and countermeasures," *Procedia Comput. Sci.*, vol. 177, pp. 503–508, 2020.
[62] N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, Funchal, Portugal: IEEE, Jul. 2017, pp. 1–7. doi: 10.1109/IoTGC.2017.8008970.

[63] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018.
[64] R. Sachdev, "Towards Security and Privacy for Edge AI in IoT/IoE based Digital Marketing Environments," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, Paris, France: IEEE, Apr. 2020, pp. 341–346. doi: 10.1109/FMEC49853.2020.9144755.
[65] T. Fernández-Caramés and P. Fraga-Lamas, "Towards The Internet-of-Smart-Clothing: A Review on IoT Wearables and Garments for Creating Intelligent Connected E-Textiles," *Electronics*, vol. 7, no. 12, p. 405, Dec. 2018, doi: 10.3390/electronics7120405.
[66] K. Xu and H. Zhu, Eds., *Wireless algorithms, systems, and applications: 10th international conference, WASA 2015, Qufu, China, August 10 - 12, 2015 ; proceedings*. in Lecture notes in computer science, no. 9204. Cham: Springer, 2015.
[67] A. H. Mohammed, Raad. M. Khaleefah, M. K. Hussein, and I. Amjad Abdulateef, "A Review Software Defined Networking for Internet of Things," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey: IEEE, Jun. 2020, pp. 1–8. doi: 10.1109/HORA49412.2020.9152862.
[68] M. A. Tunc, E. Gures, and I. Shayea, "A Survey on IoT Smart Healthcare: Emerging Technologies, Applications, Challenges, and Future Trends," 2021, doi: 10.48550/ARXIV.2109.02042.
[69] M. Kumaresan, R. Gopal, M. Mathivanan, and T. Poongodi, "Amalgamation of blockchain, IoT, and 5G to improve security and privacy of smart healthcare systems," in *Blockchain Applications for Healthcare Informatics*, Elsevier, 2022, pp. 283–312. doi: 10.1016/B978-0-323-90615-9.00015-3.
[70] I. O. Ebo, O. J. Falana, O. Taiwo, and B. A. Olumuyiwa, "An Enhanced Secured IOT Model for Enterprise Architecture," in *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, Ayobo, Ipaja, Lagos, Nigeria: IEEE, Mar. 2020, pp. 1–6. doi: 10.1109/ICMCECS47690.2020.247112.
[71] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1686–1721, 2020.
[72] L. F. A. Roman and P. R. L. Gondim, "Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment," *Ad Hoc Netw.*, vol. 97, p. 102004, Feb. 2020, doi: 10.1016/j.adhoc.2019.102004.
[73] V. Skwarek, "Blockchains as security-enabler for industrial IoT-applications," *Asia Pac. J. Innov. Entrep.*, vol. 11, no. 3, pp. 301–311, Dec. 2017, doi: 10.1108/APJIE-12-2017-035.
[74] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future Gener. Comput. Syst.*, vol. 83, pp. 326–337, 2018.
[75] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Security Challenges and Concerns of Internet of Things (IoT)," in *Cyber-Physical Systems: Architecture, Security and Application*, S. Guo and D. Zeng, Eds., in EAI/Springer Innovations in Communication and Computing. , Cham: Springer International Publishing, 2019, pp. 153–185. doi: 10.1007/978-3-319-92564-6_7.
[76] D. Prat *et al.*, "CHEM21 selection guide of classical- and less classical-solvents," *Green Chem.*, vol. 18, no. 1, pp. 288–296, 2016, doi: 10.1039/C5GC01008J.

[77] S. I. Al-Sharekh and K. H. Al-Shqeerat, "Security challenges and limitations in IoT environments," *Int J Comput Sci Netw Secur*, vol. 19, no. 2, pp. 193–199, 2019.
[78] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016, doi: 10.1109/ACCESS.2016.2549047.
[79] H. R. Dananjaya, M. Fabio, and M. Fakhrezzy, "Coordination of Global Approach for Blockchain Supply Chains," *Blockchain Front. Technol.*, vol. 2, no. 1, pp. 72–83, Aug. 2022, doi: 10.34306/bfront.v2i1.116.
[80] S. K. Singh, C. Lee, and J. H. Park, "CoVAC: A P2P smart contract-based intelligent smart city architecture for vaccine manufacturing," *Comput. Ind. Eng.*, vol. 166, p. 107967, Apr. 2022, doi: 10.1016/j.cie.2022.107967.
[81] A. Jain and T. Singh, "Security Challenges and Solutions of IoT Ecosystem," in *Information and Communication Technology for Sustainable Development*, vol. 933, M. Tuba, S. Akashe, and A. Joshi, Eds., in Advances in Intelligent Systems and Computing, vol. 933. , Singapore: Springer Singapore, 2020, pp. 259–270. doi: 10.1007/978-981-13-7166-0_25.
[82] C. Patel and N. Doshi, "Security Challenges in IoT Cyber World," in *Security in Smart Cities: Models, Applications, and Challenges*, A. E. Hassanien, M. Elhoseny, S. H. Ahmed, and A. K. Singh, Eds., in Lecture Notes in Intelligent Transportation and Infrastructure. , Cham: Springer International Publishing, 2019, pp. 171–191. doi: 10.1007/978-3-030-01560-2_8.
[83] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.
[84] K. Tabassum, A. Ibrahim, and S. A. El Rahman, "Security issues and challenges in IoT," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, IEEE, 2019, pp. 1–5. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8716460/
[85] E. Bertino, "Data privacy for IoT systems: Concepts, approaches, and research directions," in *2016 IEEE International Conference on Big Data (Big Data)*, Washington DC,USA: IEEE, Dec. 2016, pp. 3645–3647. doi: 10.1109/BigData.2016.7841030.
[86] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, IEEE, 2014, pp. 417–423. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7001385/
[87] S. Park, E. Rosca, and N. Agarwal, "Driving social impact at the bottom of the Pyramid through the internet-of-things enabled frugal innovations," *Technovation*, vol. 118, p. 102381, Dec. 2022, doi: 10.1016/j.technovation.2021.102381.
[88] A. Vaseashta, "Emerging sensor technologies for monitoring water quality," in *Applications of Nanomaterials for Water Quality*, Unitec House, 2 Albert Place, London N3 1QB, UK: Future Science Ltd, 2013, pp. 66–84. doi: 10.4155/ebo.13.208.
[89] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[90] R. Strong, J. T. Wynn, J. R. Lindner, and K. Palmer, "Evaluating Brazilian Agriculturalists' IoT Smart Agriculture Adoption Barriers: Understanding Stakeholder Salience Prior to Launching an Innovation," *Sensors*, vol. 22, no. 18, p. 6833, Sep. 2022, doi: 10.3390/s22186833.
[91] R. El-Haddadeh, V. Weerakkody, M. Osmani, D. Thakker, and K. K. Kapoor, "Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement," *Gov. Inf. Q.*, vol. 36, no. 2, pp. 310–320, Apr. 2019, doi: 10.1016/j.giq.2018.09.009.
[92] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *J. Supercomput.*, vol. 77, no. 12, pp. 14053–14089, Dec. 2021, doi: 10.1007/s11227-021-03825-1.
[93] A. Haddud, A. DeSouza, A. Khare, and H. Lee, "Examining potential benefits and challenges associated with the Internet of Things integration in supply chains," *J. Manuf. Technol. Manag.*, vol. 28, no. 8, pp. 1055–1085, Oct. 2017, doi: 10.1108/JMTM-05-2017-0094.
[94] J. Ahern, "From fail-safe to safe-to-fail: Sustainability and resilience in the new urban world," *Landsc. Urban Plan.*, vol. 100, no. 4, pp. 341–343, Apr. 2011, doi: 10.1016/j.landurbplan.2011.02.021.
[95] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, p. 100227, 2020.
[96] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet Things*, vol. 15, p. 100420, 2021.
[97] W. Ferrell, K. Ellis, P. Kaminsky, and C. Rainwater, "Horizontal collaboration: opportunities for improved logistics planning," *Int. J. Prod. Res.*, vol. 58, no. 14, pp. 4267–4284, Jul. 2020, doi: 10.1080/00207543.2019.1651457.
[98] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," *Future Internet*, vol. 12, no. 9, p. 157, Sep. 2020, doi: 10.3390/fi12090157.
[99] A. Scarfò, "The cyber security challenges in the IoT era," in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, Elsevier, 2018, pp. 53–76. Accessed: Mar. 29, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128113738000033
[100] M. Thibaud, H. Chi, W. Zhou, and S. Piramuthu, "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review," *Decis. Support Syst.*, vol. 108, pp. 79–95, Apr. 2018, doi: 10.1016/j.dss.2018.02.005.
[101] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and Secure Service Delivery," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–7, Dec. 2016, doi: 10.1145/3013520.
[102] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, 2019.
[103] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and Secure Service Delivery," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–7, Dec. 2016, doi: 10.1145/3013520.
[104] X. Yu, B. Nguyen, and Y. Chen, "Internet of things capability and alliance: Entrepreneurial orientation, market orientation and product and process innovation," *Internet Res.*, vol. 26, no. 2, pp. 402–434, Apr. 2016, doi: 10.1108/IntR-10-2014-0265.

[105] H. Jamali-Rad and X. Campman, "Internet of Things-based wireless networking for seismic applications: IoT-based wireless networking," *Geophys. Prospect.*, vol. 66, no. 4, pp. 833–853, May 2018, doi: 10.1111/1365-2478.12617.
[106] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020, doi: 10.3390/app10124102.
[107] L. Belli *et al.*, "IoT-Enabled Smart Sustainable Cities: Challenges and Approaches," *Smart Cities*, vol. 3, no. 3, pp. 1039–1071, Sep. 2020, doi: 10.3390/smartcities3030052.
[108] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Abu Dhabi, United Arab Emirates: IEEE, Oct. 2015, pp. 163–167. doi: 10.1109/WiMOB.2015.7347956.
[109] S. Aggarwal and N. Kumar, "Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges," *Comput. Commun.*, vol. 149, pp. 270–299, Jan. 2020, doi: 10.1016/j.comcom.2019.10.014.
[110] F. P. Carvalho, "Pesticides, environment, and food safety," *Food Energy Secur.*, vol. 6, no. 2, pp. 48–60, May 2017, doi: 10.1002/fes3.108.
[111] J. Shi, "Research on Optimization of Cross-Border e-Commerce Logistics Distribution Network in the Context of Artificial Intelligence," *Mob. Inf. Syst.*, vol. 2022, pp. 1–11, Aug. 2022, doi: 10.1155/2022/3022280.
[112] Y. Sutcu, Q. Li, and N. Memon, "Secure Biometric Templates from Fingerprint-Face Features," in *2007 IEEE Conference on Computer Vision and Pattern Recognition*, Minneapolis, MN, USA: IEEE, Jun. 2007, pp. 1–6. doi: 10.1109/CVPR.2007.383385.
[113] A. Kumari and S. Tanwar, "Secure data analytics for smart grid systems in a sustainable smart city: Challenges, solutions, and future directions," *Sustain. Comput. Inform. Syst.*, vol. 28, p. 100427, Dec. 2020, doi: 10.1016/j.suscom.2020.100427.
[114] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, May 2016, doi: 10.1016/j.jnca.2016.03.006.
[115] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure State Estimation and Control of Cyber-Physical Systems: A Survey," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021, doi: 10.1109/TSMC.2020.3041121.
[116] W. Steffen *et al.*, "The Anthropocene: From Global Change to Planetary Stewardship," *AMBIO*, vol. 40, no. 7, pp. 739–761, Nov. 2011, doi: 10.1007/s13280-011-0185-x.
[117] Y. Zhou, "The Application Trend of Digital Finance and Technological Innovation in the Development of Green Economy," *J. Environ. Public Health*, vol. 2022, pp. 1–8, Jul. 2022, doi: 10.1155/2022/1064558.
[118] I. Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Netw.*, vol. 129, pp. 444–458, Dec. 2017, doi: 10.1016/j.comnet.2017.09.003.
[119] A. Heiskanen, "The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity," *Constr. Res. Innov.*, vol. 8, no. 2, pp. 66–70, Apr. 2017, doi: 10.1080/20450249.2017.1337349.

[120] N. Petrovsky and J. C. Aguilar, "Vaccine adjuvants: Current state and future trends," *Immunol. Cell Biol.*, vol. 82, no. 5, pp. 488–496, Oct. 2004, doi: 10.1111/j.0818-9641.2004.01272.x.
[121] A. K. Biswas and C. Tortajada, "Water quality management: a globally neglected issue," *Int. J. Water Resour. Dev.*, vol. 35, no. 6, pp. 913–916, Nov. 2019, doi: 10.1080/07900627.2019.1670506.
[122] M. O. Harhay, "Water Stress and Water Scarcity: A Global Problem," *Am. J. Public Health*, vol. 101, no. 8, pp. 1348–1349, Aug. 2011, doi: 10.2105/AJPH.2011.300277.