International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13 Issue 5, May, 2024, Impact Factor: 8.285

Internet of Things Security: Challenges, Strategies and Implications for Cybersecurity

Reeta Singh[1], Mahesh Mahajan[2], Susheel Kumar Tiwari[3]

[1,3]Department of Computer Science & Engineering, Madhyanchal Professional University, Bhopal (M.P.), India
[2]SVKM's Institute of Technology, Dhule(M.S.), India

ABSTRACT

The Internet of Things or IoT devices' prolific spread has indefinitely changed and improved people's day-to-day lives, while also exposing society to new cybersecurity issues. This paper examines the multi-dimensional nature of securing the IoT with respect to the most critical challenges, approaches and consequences for cybersecurity. The security challenges with IoT-related devices stem from their very operational characteristics itself, consisting of diversity, resource constraints, and absence of security protocols. The more IoT security entails technical issues, the more it extends into new dimensions of legal, regulatory, and ethical values. Policy actions must be introduced to develop a minimum security regulation for IoT devices, and manufacturer should be incentivized to focus on security, and information system should be designed with transparent function. Furthermore, collaboration of stakeholders through sharing threat intelligence and application of best practices in IoT security is an important element to take care of.

Keywords: IoT, cybersecurity, authentication, authorization, encryption.

INTRODUCTION

All that the Internet of Things, or IoT, is a network of actual physical items or devices. These devices have the ability to exchange data without requiring human intervention. IoT devices may be anything with a detector and a unique identifier (UID); Machines and computers are not the only kinds of IoT devices. The primary goal of the Internet of Things is to design, develop or create secure devices that can able to communicate with each other and humans in real time. Security assurance is one of the main challenges posed by the Internet of Things [1].

History of Internet of Things (IoT)

1970s: First wireless networks were created.
1980s: Mobile devices are introduced and wireless data transfer was possible with the help of commercial cellular network.
1990s: Wearable computers and smart home appliances were appeared.
2000s: Linking between number of devices were possible with the help of broadband internet and wireless networks. Use of IoT technologies begun in the field of healthcare and manufacturing.
2010s: Household devices, like Amazon echo were introduced.
2020s: As 5G networks start to roll out and new uses for IoT technology appear on a regular basis, the IoT environment is still changing.

Significance of IoT in modern society

IoT is gradually taking on greater significance in our lives and is pervasive in our surroundings [2]. Controlling of processes and linkages of devices on the Internet of Things helped automate sectors like manufacturing, shipping and healthcare. Human lives are now better off because the Internet of Things facilitated proper operation of appliances that are remotely controlled from miles away such as the lighting, security systems and thermostats. Because of the Internet of Things, wearable medical devices that help track the vital signs and provide physicians with information in real time has been made possible, allowing them to give patients with better treatment. IoT might be widely used to prevent such a vast amount of wastes and energy conservation with the assistance of devices that could be used to monitor resource production and transferring them effectively without such a high number of emissions. For instance, smart technology use in the smart home can relate to reduced energy consumption while, smart city technology uses in improving public transport may lead to decreased traffic and air pollution. Smart homes, wearable technology, and industrial automation are just a few of the new business prospects that IoT has brought us. These opportunities have boosted the economy and

produced jobs. Individual to individual IoT-connected gadgets will present new opportunities for start-ups to build cutting-edge internet ecosystems using software development, 5G, AI, and ML.
Numerous aspects of our everyday life are changing as a result of the Internet of Things (IoT) [3]. IoT applications will completely transform a variety of businesses in the era of Industry 4.0 and 6G connectivity [4].

Emergence of cybersecurity challenges in the IoT landscape
Cybersecurity pertains to safeguarding devices, software, and data as well as the methods used to gain access to systems [5]. Cybercriminals execute intricate attacks with the use of offensive cybersecurity technology [6]. Every linked device, from industrial control systems to smart homes, is a possible target for malicious assaults. The development of comprehensive security standards and protocols has lagged behind the Internet of Things' rapid speed of development.

A lot of IoT devices are put on the market without being properly tested for security or following best practices. The absence of uniform security protocols presents notable obstacles for enterprises seeking to ensure the secure implementation of IoT technologies. IoT device data generation generates enormous amounts of data, which poses issues with data privacy and regulatory compliance.

Purpose of the research
These research papers aim to investigate, examine, and offer insights into many facets of Internet of Things (IoT) security, with an emphasis on cybersecurity consequences, tactics, and issues such as identifying and analyzing the challenges, examining current strategies, assessing the implications for cybersecurity etc.

Architecture of IoT
In most cases, the architecture of the IoT have several layers, with each layer assigned specific roles in order to facilitate the connections, communications, and interactions involving devices and systems. The following fig. 1 shows the five-layer architecture of IoT.

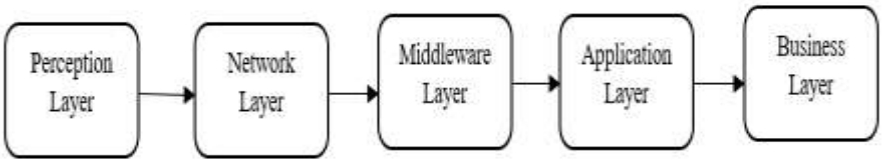

Fig. 1. Five Layer Architecture of IoT

Perception Layer: This layer can be divided into two subgroups: sensors, actuators, and other devices that directly interact with the physical world, and the cloud, networks, data analytics, and other intelligent software that manages operations remotely. Sensors extract data from the external environment (e.g., temperature, humidity, motion), while actuators make it possible for devices to perform tasks, and they can switch on/off, or change the settings. Its primary duty is to identify the object while acquiring data [7].

Network Layer: Everything, including servers and network devices, is connected by a network layer [8]. The network layer is the one performing the task of making IoT devices achieve their communication process and, possibly, data transmitted to where it is required. This layer consists of networking technologies like Wi-Fi, Bluetooth, Zigbee, LoRa, cellular networks, and so on. Besides, these gateways are used to link wireless protocols of different types.

Middleware Layer: The application layer offers interfaces and protocols that take care of data transmission between the Internet of Things devices. It comprises details including data ingestion, message queuing, data processing, and protocol translation, as an example. Middleware could be programmed to perform such functions as device management, security, and authentication as well.

Application Layer: The application layer comprises services, applications, and other agents that derive specific capabilities from IoT data. Such applications may cover the entire range of consumer smart home solutions to industrial automation systems, as well as healthcare monitoring, environmental monitoring, and others. End users can communicate with all of the linked devices through this layer [8].

Business Layer: The business layer in IoT architecture links device data with organizational flows, where the data processing is done, insights are extracted, and production rules are applied to take advantage of them. It provides functions such as device lifecycle management, data integration, and security of events. This is a function that helps organizations with many aspects of functional operations such as decision-making, operational efficiency, and business innovation by exploiting data-driven insight and automating processes.

Challenges in Securing IoT

The Internet of Things, or IoT, has grown rapidly to become a major influence on how people live, work, and communicate. Globally, there are increasing numbers of internet-enabled devices, changing global rights just the way we live. The topic of Internet of Things comes with many challenges. Additionally, the Internet of Things will expand the areas that hackers and other cybercriminals could potentially target [9].

1.1 **Absence of encryption:** The fact that IoT is secure from classifying the encryption is to keep it away from hackers who can easily access the database. With a level of processing and storage similar to that of traditional computers, these hackers can function like them. Security measures for Internet of Things devices include well-known symmetric and asymmetric encryption techniques [10].

1.2 **Inadequate testing and upgrading:** Unfortunately, manufacturers of IoT devices offering mass production, selling, and shipping increase more competitions and care less about security details that are related to the device. IoT devices that must have direct Internet connectivity should be divided into their own network segment and have access to other networks restricted in order to increase security [11].

1.3 **Inadequate device security:** This can be caused by a variety of security pitfalls, such as obsolete software, weak passwords, unpatched vulnerabilities, and a lack of encryption. To cover the security of sensitive data stored in these devices, it's critical to modernize the software frequently and put in place robust security measures. The lot of IoT devices are readily hackable and have lax security measures.

1.4 **Absence of standardization:** In a certain sector or area, lack of standardization is defined as the absence of established norms or conditions. This may lead to inconsistencies across different products, systems, or processes, which would be hamstrung and cause confusion as well as a reduction in interoperability.

1.5 **Vulnerability to network intrusions:** "Vulnerability to network attacks" refers to how simple it's for hackers to breach or take advantage of a system, network, or device. Unpatched software, poor word operation, network armature faults, or a poor security setup can each contribute to this. Fiscal loss, data theft, or service outages are all possible issues of network attacks. In networks, the larger the network, the higher the likelihood of an attack [12].

1.6 **Transmission of data without security:** "Unsecured data transmission" refers to data that is transmitted via a network or the internet but is not appropriately protected. This suggests that the data may be intercepted, altered, or stolen by hackers. Unsecure data transmission occurs when information is sent via insecure protocols or over an unprotected network connection. Ensuring that electronic data is protected from unauthorized access, contamination, and theft over its whole lifecycle is known as data security [13].

1.7 **Privacy concerns:** These issues relate to the collection, storage, application, and sharing of particular information.

1.8 **Software weaknesses:** Software vulnerabilities are gaps or exceptions in the law that a hacker may exploit to gain unauthorized access, steal sensitive information, or carry out other destructive deeds. Software vulnerabilities can arise from crimes or excrescences made during the creation process, as well as by exercising outdated or unsubstantiated software. Hackers might use these vulnerabilities to take over a computer, install malware, or steal particular information.

LITERATURE REVIEW

The authors [1] provide a review of the current state of anomalies and security concepts in IoT. It also categorizes and evaluates the most common security concerns with the layered architecture of the Internet of Things, taking into account management protocols, connections, and communication. The study [8] examines IoT security concerns and draws attention to related challenges. The authors [9] review the several issues and challenges of IoT and also discussed IoT solutions proposed by industry experts, academic experts, and technicians.

The authors [14] reviewed and presented IoT security threats from different perspectives, like hardware, software, and data in transit. The paper also demonstrates ML and Blockchain technologies and their effect on security when utilized in an Internet of Things platform. In their paper [11], the authors provide a summary of the threats that have been found and suggest ways to keep the Internet of Things safe going forward. In their paper [12], the authors study security or privacy issues using Machine Learning algorithms or Blockchain techniques. They also categorize various security and privacy threats in the IoT and discussed solutions using ML algorithms and Blockchain techniques. The study [15] uses a Blockchain-based, multi-level architectural distributed security model for Internet of Things devices that communicate over multi-hop cellular networks.

Strategies for IoT Security

IoT security is based on a cybersecurity approach to protect connected devices from cyberattacks and the weak networks they connect to. There is no built-in security with the IoT. Because IoT-related devices operate without being noticed by traditional cybersecurity systems and transport data over the internet without encryption, IoT security is required to protect data. Following fig. 2 shows the common strategies for IoT security.

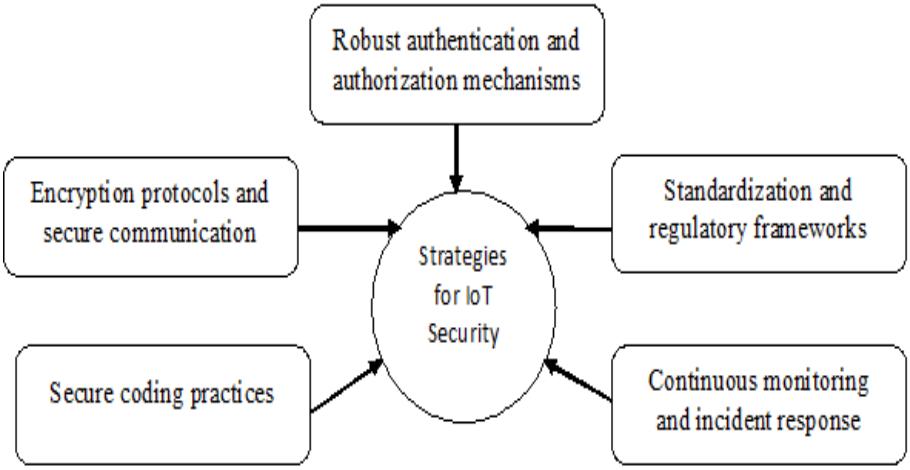

Fig. 2. Strategies for IoT Security

Robust authentication and authorization mechanisms: Robust authentication processes, similar part-grounded access control, and multifactor authentication (MFA) are needed for IoT devices. One system to do this is to combine passwords and biometrics. Authentication is a crucial security requirement for Internet of Things devices [16]. Three factors are typically taken into account when evaluating the performance of authentication schemes: security, computing overhead, and communication overhead [17].

Multifactor Authentication (MFA): MFA, or multi-factor authentication, is a very powerful method for enhancing security of IoT devices. By utilizing two or more verification methods, such as a password, security token, or fingerprint, multi-factor authentication (MFA) significantly raises the control for unauthorized users to get access. MFA increases the barrier to entry for hackers by introducing an extra layer of security to IoT devices. Even if someone were to be able to crack your password, MFA would still require the second verification method in order to provide access to the device. Numerous businesses use MFA in order to abide by security regulations. The contents of IoT packets are represented by a unique one-way digital fingerprint created by the multifactor authentication technique [18].

Role-Based Access Control (RBAC): To secure both IoT devices and data, role-based access control is important. The intended protection against illegal use of the available resources is provided by access control [19].

Encryption protocols and secure communication: The first step in guarding Internet of Things systems is to ensure that data stored on devices and in the cloud uses protocols that perform encryption operations at the presentation layer. Certain interdependencies, such as Open SSL or SSH servers, may be especially vulnerable to attacks in particular environments where they might give unauthorized parties access to non-public data. It's essential to choose interdependency performances with the least quantum of vulnerability to this threat. Using cryptographic bias for data encryption procedures, similar to TPMs or HSMs, is the topmost way to ameliorate cyber security on the Internet of Things. By encrypting the data using encryption algorithms that conceal the information, cryptography is necessary to provide secure data exchange via networks [20].

Strong encryption standards: Algorithms for encryption are employed to guarantee confidentiality [21]. To guarantee data security on the Internet of Things, choosing the appropriate encryption system is essential. Every encryption system has advantages and disadvantages of its own; thus, it's critical to elect the algorithm that meets the demands of the particular operation. The Advanced Encryption System (AES) is a popular encryption system that has a strong security character and good performance. The US civil government uses it to guard sensitive data. Another well-liked public and private crucial encryption system is Rivest-Shamir-Adleman (RSA). Digital signatures and secure data transfer are two uses for it. Another encryption system that secures data with three rounds of encryption is called Triple Data Encryption Standard, or Triple DES. It's employed in operations that demand a high degree of security.

End-to-end encryption in IoT communication: End-to-end encryption, or E2EE, acts as a firewall to save the sequestration of digital dispatches. It's a secure security point that ensures dispatches remain non-public and are only viewable by the intended recipients. Data is translated at the sender's end and is only decrypted by the intended recipient to prevent unauthorized parties from penetrating or reading it while it's in transit. The transport layer manages end-to-end communication on the Internet of Things. One secure communication technique is end-to-end encryption, or E2EE, which safeguards information while it's being transferred [22].

Secure coding practices: It is necessary to follow secure rendering guidelines and best practices. Need to avoid hard-coded credentials and sensitive information in the code and conduct static and dynamic code analysis to identify and fix security vulnerabilities.

Importance of secure development lifecycle: One descriptive and prescriptive aspect of software development is the software lifecycle [23]. The Secure Development Lifecycle (SDL) is a set of practices and processes designed to integrate security measures into every phase of the software development process. For IoT devices, where security enterprises are particularly critical due to the implicit impact on both user privacy and physical systems, espousing a secure development lifecycle is of consummate significance. SDL helps identify and address security issues beforehand in the development process, reducing the liability of vulnerabilities making their way into the final product. SDL involves thorough troubleshooting to identify implicit security pitfalls and vulnerabilities specific to the IoT device.

Addressing common vulnerabilities in IoT software: Need to design APIs with security in mind, using proper authentication and authorization. By addressing common vulnerabilities and espousing a comprehensive security approach throughout the development lifecycle, IoT software can become more flexible to implicit risks and better cover the insulation and security of users and their data. There is a great deal of uncertainty in the requirements specifications related to the software development process for Internet of Things systems [24].

Standardization and regulatory frameworks: In order to guarantee the compatibility, security, and responsibility of IoT (Internet of Things) systems and various devices, standardization and legal frameworks are pivotal. Around the world, a number of associations and non-supervisory authorities are working to produce norms and laws to overcome the difficulties brought on by the different and rapidly changing IoT ecosystem. We need to develop international morals to ensure the quality, safety, and effectiveness of products and services, including those related to IoT. Need to develops rules for different aspects of IoT, including communication protocols, security, and device interoperability. Different industries, such as healthcare, automotive, and energy, must implements specific regulations governing the use of IoT technologies within their disciplines. Due to the lack of standards in many IoT-based smart settings, malicious software can infiltrate IoT devices with ease via trusted boot, firmware upgrades, and device acquisition, in addition to services and apps [25].

Development of IoT security standards: The development of IoT (Internet of Things) security norms is a cooperative and ongoing process involving multiple associations, normative bodies, stakeholders from various industries, and regulatory agencies. Establishing comprehensive security rules and norms is vital to addressing the different and evolving challenges associated with the deployment of IoT-related devices. Need to identify and dissect the unique security conditions and challenges associated with IoT-related various devices and systems. This includes considerations for device authentication, data protection, secure communication, and device lifecycle operation. A standard for IoT security is proposed and made public both by IETF and IEEE.

Regulatory compliance for IoT manufacturers: Regulatory compliance is vital for IoT (Internet of Things) manufacturers to ensure the security, insulation, and safety of IoT related devices. Compliance with applicable regulations also helps make trust among consumers, minimizes legal risks, and promotes responsible business practices. The nonsupervisory landscape for IoT may vary by region and industry-wise, but several common considerations live. IoT devices should be designed with robust security features, including secure boot, encryption, secure firmware updates, and strong authentication mechanisms. When gathering, using, and storing particular data via IoT devices, associations need to get the right concurrence and abide by laws. The users should be informed about the extent, and retention of data acquired through the establishment of clear sequestration rules and open data handling procedures.

Continuous monitoring and incident response: Given the dynamic nature of IoT security threats, nonstop monitoring and incident response capabilities are pivotal. Organizations should establish robust monitoring systems to detect anomalies and suspicious conditioning in IoT networks. Incident response plans should be developed and tested to ensure an effective response to implicit security incidents.

Real-time threat detection: Real-time trouble discovery in the IoT (Internet of Things) involves continuously controlling, monitoring, and analyzing data from various connected IoT devices to identify and respond instantly to implicit security threats.

Implications for Cybersecurity

Different manufacturers produce IoT devices, which results in a variety of ecosystems and standards. Enforcing a uniform security posture throughout the Internet of Things (IoT) environment may be difficult due to inconsistent security procedures and standards. A lot of IoT devices use weak or default passwords, which leaves them open to hacking. The security of the ecosystem as a whole may be compromised by inefficient permission and authentication processes. A thorough approach to risk management for the Internet of Things (IoT) with an emphasis on cybersecurity concerns is necessary due to the massive volumes of daily data generated by IoT operations that are communicated with a high sensitivity to hazards and threat attacks [26]. Ensuring security means protecting IoT devices and services from unauthorized access from both inside and outside of the devices [27].

Sensitive data handling in IoT:

Because of their uniqueness, the lack of safety standards and norms, and a variety of threat vectors, Internet of Things devices are susceptible to cyberattacks [28]. Sensitive information may leak out or be breached if an IoT device processes, transmits, or stores data improperly. Attackers could use these flaws to gain harmful manipulation or unauthorized access to important data. Securing the network acting as a link between the Internet of Things devices and the back-end systems is crucial. Security technologies like firewalls, intrusion detection, antivirus, anti-malware, VPNs, and preventive systems can be put into place to do this. The best practices for handling sensitive data in the IoT are to collect only needed data, implement strong encryption, provide secure authentication, enforce access control, use secure communication protocols while transmitting data between various IoT devices and backend systems, implement a secure device identity management system, establish policies for the entire data lifecycle, etc. Each and every case of cyberattack that happens nowadays includes a massive amount of data [29].

Integration of IoT into critical infrastructure:

Organizations must assess their current IoT cyber infrastructure from both a technological and administrative standpoint in order to establish a forward-looking cyber risk management plan [30]. IoT devices, which go beyond environmental monitoring sensors to include standard office supplies and network devices, are incredibly valuable to businesses. If IoT devices in critical infrastructure networks are not adequately protected, though, there is a greater chance that unauthorized individuals may get access to networks and operational data. The hackers frequently leverage improper setups, such as default credentials and unpatched vulnerabilities, to obtain access to devices or networks. Once access is gained, attackers may use the network to locate other data, and organize extensive attacks on devices and equipment that are vulnerable. While there are numerous advantages to IoT, its integration also presents new difficulties, especially in the areas of security and trustability. More planning for adaptability is made possible by the use of the IoT in critical structures. Constant observation and data processing help in locating weak points and enhance the capacity to reply to and bounce back from disturbances.

Societal impact of IoT security breaches:

In the end, IoT might completely transform our business environment [31]. IoT based devices constantly gather and retain sensitive data, including financial data or particular information. This information might be exploited for identity theft or other lawless exertion if a hacker manages to gain access to it. Be sure that only reliable IoT grounded devices must be connected to the network. Need to avoid connecting IoT-grounded devices that did not buy from a trusted dealer. IoT-related devices gather and store vast quantities of specific data, which leaves them open to abuse and security setbacks. This might have a big effect on individual information and the protection of specific data. The first step of defense for IoT-grounded device security is device hardening and safe configuration. This makes sure that IoT related devices are configured with the latest security fixes, creating strong passwords for users, and shutting down gratuitous services. Network segmentation is another essential IoT security practice. This means segmenting the network to keep IoT-related devices piecemeal from other network-linked devices and services in order to lessen the attack face of the network.

CONCLUSION

The security of the Internet of Things poses major and very challenging issues that call for creative fixes. Strong security measures must be put in place to protect against changing cyberthreats. Working on these issues will have a significant impact on cybersecurity as a whole, particularly in light of society's growing reliance on IoT-based devices.

REFERENCES

[1]. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 2023, 23, 4117. https://doi.org/10.3390/s23084117

[2]. Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019). https://doi.org/10.1186/s40537-019-0268-2

[3]. Ghashim, I.A.; Arshad, M.Internet of Things (IoT)-Based Teaching and Learning: Modern Trends and Open Challenges.Sustainability 2023, 15, 15656. https://doi.org/10.3390/su152115656
[4]. Khan, M.Z; Alhazmi, O.H.;Javed, M.A.; Ghandorh, H.; Aloufi,K.S. Reliable Internet of Things:Challenges and Future Trends.Electronics 2021, 10, 2377. https://doi.org/10.3390/electronics10192377
[5]. Raimundo, R.J.; Rosário,A.T. Cybersecurity in the Internet of Things in Industrial Management.Appl. Sci. 2022, 12, 1598. https://doi.org/10.3390/app12031598
[6]. Kim, K.; Alfouzan, F.A.; Kim, H. Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. Appl. Sci. 2021, 11, 7738. https://doi.org/10.3390/app11167738
[7]. Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun and Hui-Ying Du, "Research on the architecture of Internet of Things," 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Chengdu, 2010, pp. V5-484-V5-487, doi: 10.1109/ICACTE.2010.5579493.
[8]. Khalaifat , W. 2024. An Overview of Iot Architecture Security Issues and Countermeasures. Asian Journal of Research in Computer Science. 17, 4 (Feb. 2024), 1–18. DOI: https://doi.org/10.9734/ajrcos/2024/v17i4427.
[9]. Aldowah, Hanan & Rehman, Shafiq & Umar, Irfan. (2019). Security in Internet of Things: Issues, Challenges, and Solutions. 10.1007/978-3-319-99007-1_38.
[10]. Aydogan, A.F., Varol, C., Rasheed, A.A., & Karpoor, N. (2023). A Review of Encryption Techniques in IoT Devices.
[11]. Balogh, S.; Gallo, O.;Ploszek, R.; Špaˇcek, P.; Zajac, P. IoTSecurity Challenges: Cloud andBlockchain, PostquantumCryptography, and EvolutionaryTechniques. Electronics 2021, 10, 2647. https://doi.org/10.3390/electronics10212647
[12]. Nazar Waheed, Xiangjian He*, Muhammad Ikram, Muhammad Usman, Saad Sajid Hashmi, and Muhammad Usman. 2020. Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. ACM Comput. Surv. 53, 3, Article 1 (April 2020), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn
[13]. Vinay Michael, & Jubilant J Kizhakkethottam. (2023). IoT and Data Security. Journal of Population Therapeutics and Clinical Pharmacology, 30(9), 283–290. https://doi.org/10.47750/jptcp.2023.30.09.028
[14]. Phillip Williams, Indira Kaylan Dutta, Hisham Daoud, Magdy Bayoumi,A survey on security in internet of things with a focus on the impact of emerging technologies,Internet of Things,Volume 19,2022,100564,ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100564.
[15]. Kiran, A.; Mathivanan, P.; Mahdal, M.; Sairam, K.; Chauhan, D.; Talasila, V. Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques. Mathematics 2023, 11, 2073. https://doi.org/10.3390/math11092073
[16]. M. Aman, K. Chua, and B. Sikdar, “Mutual authentication in IoT systems using physical unclonable functions,” IEEE Internet of Things Journal, vol. 4, pp. 1327 – 1340, 05 2017.
[17]. Zhao, J.; Hu, H.; Huang, F.; Guo, Y.; Liao, L. Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. Electronics 2023, 12, 1812. https://doi.org/10.3390/electronics12081812
[18]. Ahmed, A.A.; Ahmed, W.A. An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. Sensors 2019, 19, 3663. https://doi.org/10.3390/s19173663
[19]. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors 2023, 23, 1805. https://doi.org/10.3390/s23041805
[20]. Silva, C., Cunha, V.A., Barraca, J.P. et al. Analysis of the Cryptographic Algorithms in IoT Communications. Inf Syst Front (2023). https://doi.org/10.1007/s10796-023-10383-9
[21]. Mohammad Al-Mashhadani,Mohamed Shujaa, "IoT Security Using AES Encryption Technology based ESP32 Platform", The International Arab Journal of Information Technology (IAJIT) ,Volume 19, Number 02, pp. 214 - 223, March 2022, doi: 10.34028/iajit/19/2/8.
[22]. K.B. Sarmila, S.V. Manisekaran “A Study on Security Considerations in IoT Environment and Data Protection Methodologies for Communication in Cloud Computing”, 2019 International Carnahan Conference on Security Technology (ICCST), 1-3 Oct. 2019, DOI:10.1109/CCST.2019.8888414
[23]. Melinda, M., Ramadhan Na, S. R., Nurdin, Y., & Yunidar, Y. (2023). Implementation of System Development Life Cycle (SDLC) on IoT-Based Lending Locker Application . Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 7(4), 982 - 987. https://doi.org/10.29207/resti.v7i4.5047
[24]. Ismail, S.; Dawoud, D.W. Software Development Models for IoT. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022, Las Vegas, NV, USA, 26–29 January 2022; pp. 524–530. [CrossRef]
[25]. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
[26]. AlSalem, T.S.; Almaiah, M.A.; Lutfi, A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics 2023, 12, 3958. https://doi.org/10.3390/electronics12183958

[27]. Singh, A.; Kumar, S. Preliminary Study of The Internet of Things (IoT) and Cyber Security for Predictive Data Analytics, in Proceedings of the MOL2NET'23, Conference on Molecular, Biomed., Comput. & Network Science and Engineering, 9th ed., 25–31 December 2023, MDPI: Basel, Switzerland

[28]. Alterazi, H.A.; Kshirsagar, P.R.; Manoharan, H.; Selvarajan, S.; Alhebaishi, N.; Srivastava, G.; Lin, J.C.-W. Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. Sensors 2022, 22, 6117. https://doi.org/10.3390/s22166117

[29]. Lavanya, S. and Mythili, K. and Kannimuthu, Dr. S., An Integration of Big Data Analytics and Cyber Security-A Panoramic Survey (2020). International Journal of Advanced Research in Engineering and Technology (IJARET), 11(9), 2020, pp.747- 754, Available at SSRN: https://ssrn.com/abstract=3712184

[30]. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 2020, 12, 157. https://doi.org/10.3390/fi12090157

[31]. Radanliev, P., De Roure, C.., Cannady, S., Montalvo, R.M., Nicolescu, R., Huth, M., 2018. Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance, in: Living in the Internet of Things: Cybersecurity of the IoT - 2018. Institution of Engineering and Technology, London. https://doi.org/10.1049/cp.2018.0003