International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 06, ISSN No. 2455-2143, Pages 48-55
Published Online October 2023 in IJEAST (http://www.ijeast.com)

ENHANCING IOT SECURITY: ADDRESSING CHALLENGES, IMPLEMENTING SOLUTIONS, AND ENVISIONING CYBERSECURITY TRENDS FOR THE FUTURE

Mr J.Lalu Prasad,
Research scholar,
Department of Computer Science & Engineering,
Mohan babu University, Tirupati, Andhrapradesh,
517102, India,

Mr Ch .Parvateesam,
Assistant Professor, Dept.Of CSE,
Aditya Institute of technology and management (A),
Tekkali, Ap, India,

Mr Sayyed Nagulmeera ,
Research scholar,
Department of Computer Science & Engineering,
Mohan babu University, Tirupati,
Andhrapradesh, 517102, India,

Mr V Avinash Professor,
Assistant Professor,
Dept.Of CSE,Raghu engineering college(A),
vizag,Andhrapradesh,India,

Abstract— **The rapid growth of the Internet of Things (IoT) has revolutionized the technology landscape, interconnecting smart devices and sensors to gather data-driven insights across various industries. Nevertheless, this transformative advancement has brought about security challenges as well, with the interconnected nature of devices leaving them vulnerable to potential cyber threats and exploitation. This research paper explores the multifaceted challenges, existing solutions, and future directions in IoT cybersecurity. It identifies hurdles like resource constraints and privacy concerns, discusses strong authentication and data encryption as solutions, and envisions AI and blockchain to enhance security. By fostering collaboration among stakeholders, a safer and more resilient IoT ecosystem can be achieved, ensuring the IoT's full potential while addressing security concerns.**

Keywords— **IoT, cyber security, physical tampering, privacy concerns, Ransomware attacks, Firmware Vulnerabilities**

I. INTRODUCTION

The Internet of Things (IoT) has surfaced as a revolutionary influence. Interconnecting an extensive network of smart devices, sensors, and everyday objects, all enabled with internet connectivity. This interconnectedness has revolutionized various industries, promising unparalleled efficiency, convenience, and Insights derived from data analysis. Nevertheless, due to the rapid expansion of IoT devices in households, industries, and critical infra`structure, the imperative of safeguarding the security and privacy of this extensive ecosystem has risen significantly.

Addressing the security of the Internet of Things (IoT) poses a multifaceted and intricate challenge, given the diverse array of applications these intelligent devices cover, from smart home appliances and wearable gadgets to industrial control systems and autonomous vehicles. Each of these devices, regardless of its size or function, represents a potential entry point for cyber attackers seeking to exploit vulnerabilities, compromise data, or disrupt essential services. Moreover, the vast scale of IoT

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 06, ISSN No. 2455-2143, Pages 48-55
Published Online October 2023 in IJEAST (http://www.ijeast.com)

deployment and the heterogeneity of devices amplify the complexity of safeguarding this interconnected realm.
This research paper aims to delve into the various challenges that confront IoT security, explore existing solutions and best practices, and envision future directions in cybersecurity to create a robust and resilient IoT landscape.

Through comprehending the risks and vulnerabilities inherent in IoT ecosystems, we can forge the path towards inventive approaches that safeguard the security, privacy, and dependability of these technologies, which have seamlessly integrated into our everyday existence.

II. TYPES OF CYBER SECURITY ISSUES

Cybersecurity issues in IoT are numerous and diverse due to the wide range of interconnected devices and the complexity of IoT ecosystems. Some of the prominent types of cybersecurity issues in IoT include:

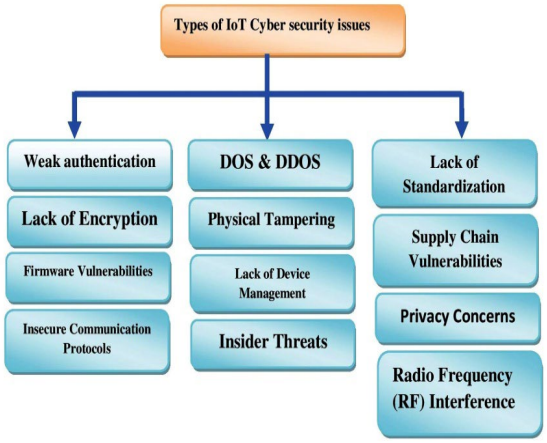

Figure 1: Types of IoT Cyber security issues**.**

III. WHAT ARE IOT CYBER SECURITY ISSUES?

Cyber security issues can have severe consequences for IoT device privacy, leading to the destruction or compromise of users' personal data and sensitive information. The following ways illustrate how cybersecurity issues can destroy IoT device privacy:
The exponential growth of the Internet of Things (IoT) gives rise to considerable cybersecurity apprehensions. As devices become more interconnected and vast amounts of data are exchanged, the potential for cyber-attacks and breaches in IoT systems becomes a significant concern.

Some of the key cybersecurity issues in IoT include:

- **Data Breaches:** The presence of cybersecurity vulnerabilities in IoT devices can result in data breaches, potentially granting unauthorized access to the data collected and transmitted by these devices. If attackers gain access to personal information, such as user identities, passwords, or financial details, they can exploit or sell this data for malicious purposes, compromising users' privacy.

- **Unauthorized Access**: Attackers can exploit weak authentication mechanisms and default credentials in Internet of Things (IoT) devices, gaining unauthorized access. Once infiltrated, they can monitor user activities, track movements, and eavesdrop on private communications, compromising users' privacy.

- **Data Interception:**Insecure communication channels can enable cyber attackers to intercept data transmitted between IoT devices and their associated servers. This interception may expose sensitive information, including user behaviors, preferences, and habits, which could be used to build detailed profiles of individuals and invade their privacy.

- **Remote Control and Manipulation:** Cybersecurity vulnerabilities in IoT devices can allow attackers to remotely take control of the devices. This can lead to unauthorized monitoring or manipulation of device functionalities, potentially compromising users' private activities and environments.

- **Identity Theft:** Cybersecurity attacks aimed at IoT devices can lead to the unauthorized acquisition of personal information. This pilfered data might be exploited for identity theft, financial fraud, or other malevolent endeavors, severely affecting users' privacy and financial well-being.
- **Surveillance and Espionage:** Compromised IoT devices can be used for unauthorized surveillance or industrial espionage. Attackers could use smart cameras or microphones in IoT devices to monitor individuals or confidential business activities, posing serious privacy threats.

- **Ransomware Attacks:** Some cybersecurity attacks on IoT devices involve ransomware, where attackers lock users out of their own devices or encrypt their data until a ransom is paid. This form of attack can not only deny users access to their devices but may also threaten to leak private data if the ransom is not paid.

- **Unauthorized Data Sharing:** Insecure IoT devices may inadvertently share users' data with unauthorized third parties due to misconfigurations or design flaws. Such data sharing can lead to privacy violations and potentially result in personal information being sold or misused.

Ensuring the privacy of IoT devices necessitates the implementation of robust security measures by manufacturers

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 06, ISSN No. 2455-2143, Pages 48-55
Published Online October 2023 in IJEAST (http://www.ijeast.com)

and developers. These measures encompass strong authentication mechanisms, data encryption, regular security updates, and strict adherence to privacy regulations. Additionally, users play a vital role in safeguarding their IoT devices by remaining vigilant about changing default credentials, updating firmware, and being aware of potential security risks when integrating these devices into their homes or workplaces.

IV. TYPES OF CYBERSECURITY ISSUES AND ATTACKS

A. **Weak Authentication:** Many IoT devices come with default or weak credentials, making them susceptible to unauthorized access. Attackers can exploit this weakness to compromise devices and gain control over the entire IoT network.

Figure 2: Weak authentication. In secure Communication: Certain IoT devices utilize insecure communication protocols, making data vulnerable to interception and manipulation. Insufficient encryption during data transmission can result in data breaches and violations of privacy.

B. **Firmware Vulnerabilities**: IoT devices frequently incorporate firmware that might harbor security vulnerabilities. Without prompt updates and patches, these vulnerabilities can be exploited by attackers to gain unauthorized access.
C. **Lack of Encryption:** Inadequate data encryption between IoT devices and servers can result in sensitive information being exposed to eavesdropping and unauthorized access.
D. **DDoS and DoS Attacks:** IoT devices can be compromised and used as part of botnets to launch DoS and DDoS attacks, leading to service disruptions.
E. **Physical Tampering:** Physical access to IoT devices can allow attackers to tamper with them, extract sensitive information, or inject malicious code.
F. **Privacy Concerns:** The substantial volume of data gathered by IoT devices raises privacy concerns, particularly when the data is mishandled or utilized without users' consent.
G. **Lack of Device Management:** Improper device management can result in unauthorized access, uncontrolled device behavior, and difficulties in detecting compromised devices.
H. **Insider Threats:** Employees or individuals with authorized access to IoT devices can pose a threat to security by intentionally or unintentionally misusing devices or data.
I. **Weaknesses in the supply chain:** IoT devices are typically produced by various vendors and may include components with security vulnerabilities.Attackers could exploit these vulnerabilities to compromise the entire IoT system.
J. **Radio Frequency (RF) Interference:** Some IoT devices may use wireless communication technologies susceptible to RF interference, leading to data corruption or communication disruption.

K. **Lack of Standardization:** The absence of standardized security protocols across IoT devices can create compatibility issues and result in varying levels of security, making it difficult to establish a unified security framework.

Addressing these cyber security issues requires a comprehensive and collaborative approach involving manufacturers, consumers, policymakers, and security professionals. To fortify IoT security and ensure the secure and dependable functioning of interconnected systems, it is crucial to implement robust authentication, encryption, regular updates, and secure communication protocols.

V. POTENTIAL BENEFITS AND COST OF CYBER CRIME

The convergence of cybersecurity and the Internet of Things holds the potential for numerous benefits. These benefits include improved data security and privacy, enhanced operational efficiency, increased productivity, and the creation of new business opportunities. Enhancing cybersecurity in the IoT can offer a significant advantage by bolstering data security and privacy. As the number of IoT devices collecting and exchanging data continues to rise, there is a mounting concern regarding the security and privacy of this data.Cybersecurity measures can address these concerns by implementing strong authentication and encryption protocols, implementing secure communication channels, and establishing robust access controls. Another potential benefit of cybersecurity in the IoT is enhanced operational efficiency. By implementing effective cybersecurity measures, Organizations can reduce the risk of cyber-attacks and unauthorized access to IoT devices through various mitigation strategies.This can help maintain the smooth functioning of critical systems and prevent disruptions to operations. Furthermore, cybersecurity in the IoT can increase

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 06, ISSN No. 2455-2143, Pages 48-55
Published Online October 2023 in IJEAST (http://www.ijeast.com)

productivity. By prioritizing the security and integrity of IoT devices and systems, organizations can minimize the downtime caused by cyber-attacks or system compromises. This can lead to increased productivity, as employees can continue working without interruption and access to critical data and resources is maintained. Additionally, the convergence of cybersecurity and the IoT can create new business opportunities.

From the source of: (https://purplesec.us/resources/cyber-security-statistics/)

- The COVID-19 pandemic has led to a significant surge in cybercrime, witnessing a staggering increase of 600%.
- By the year 2025, global cybercrimes are projected to incur a staggering annual cost of $10.5 trillion
- The annual cost of cybercrime worldwide is approximately $6 trillion, according to estimates
- The economic repercussions of cybercrime are equivalent to approximately 1% of the Global GDP.
- On average, a malware attack results in a cost exceeding $2.5 million for a company, considering the time and resources required to address and mitigate the aftermath of the attack.
- In 2021, the destructive impact of ransomware has surged to 57 times its level in 2015.
- Between 2018 and 2020, more than two-thirds (66%) of the approximately 30 million small and medium-sized businesses (SMBs) in the United States encountered at least one incident.

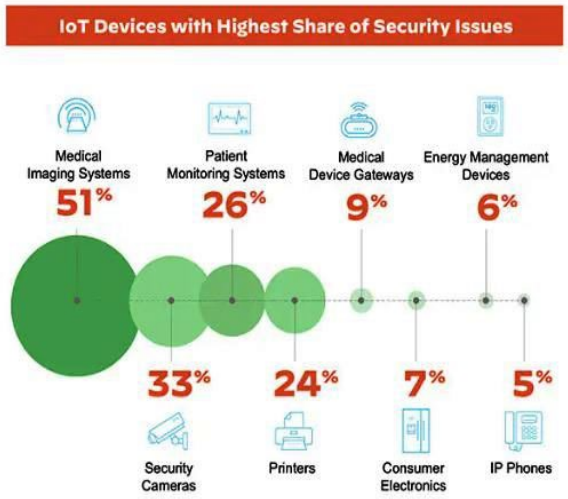

Figure 3: The most significant proportion of security concerns. Source (https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security)

- On average, small businesses encounter data breach costs ranging from $120,000 to $1.24 million.
- In 2021, there was a substantial increase in the average total cost of data breaches, reaching $4.24 million, marking the highest value ever recorded in the 17-year history of this report. This represents a notable rise compared to the previous year's cost of $3.86 million.
- Data breaches that were influenced by remote work as a contributing factor incurred an average cost that was $1.07 million higher than breaches not involving such a factor.
- Security Driven AI demonstrated the most effective cost mitigation, leading to savings of up to $3.81 million, which accounts for an impressive 80% difference in costs compared to other approaches.).
- The implementation of zero trust security policies led to cost savings of $1.76 million per breach.
- From 2020 to 2021, the average total cost of a breach experienced a 10% increase.
- The cost of a breached record containing Personally Identifiable Information (PII) amounts to $180.
- Over 50% of all cyber attacks are borne by small and medium-sized businesses (SMBs).
- Enterprises, on average, experienced 130 security breaches per year, per organization.
- In 2021, enterprises experienced a notable 22.7% rise in the annual cost of cybersecurity.
- The yearly count of security breaches on enterprise organizations rose by 27.4%
- Enterprise organizations, on average, required 50 days to resolve an insider's attack and 23 days to recover from a ransomware attack.
- Approximately 71.1 million individuals become victims of cybercrimes each year.
- On average, individuals suffer losses of $4,476 USD.
- Cybercrime causes individuals to lose a substantial sum of $318 billion.
- On average, individuals who fall victim to phishing scams incur losses of $225.

The top five cybercrimes in 2021 were:

- **Extortion-** is the illegal practice of obtaining something, often money or other valuables, from someone through coercion, threats, or intimidation.
- **Identity theft-** is the fraudulent act of stealing someone's personal information, such as their name, social security number, financial details, or other identifying data, with the intention of assuming that person's identity for deceptive purposes, often to commit financial fraud or other crimes.
- **A personal data breach**- involves unauthorized access or disclosure of sensitive information, potentially leading to privacy risks for affected individuals.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 06, ISSN No. 2455-2143, Pages 48-55
Published Online October 2023 in IJEAST (http://www.ijeast.com)

- **Non-payment** -refers to the failure or refusal to make a required payment, often resulting in financial consequences or contractual disputes.
- Phishing attacks deceive individuals into sharing sensitive information by posing as trustworthy entities through emails, websites, or messages.
- Gaining full access to an individual's entire online identity is valued at approximately $1,000.
- Personal Identifiable Information (PII) is valued at approximately $200 per record.
- For just $50, individuals can acquire both malware and a comprehensive tutorial on how to use it.
- Through a monthly investment of $34, a criminal could potentially earn $25,000 per month.

VI. CHALLENGES IN IOT CYBER SECURITY

IoT (Internet of Things) cybersecurity faces a multitude of challenges due to the unique nature of interconnected smart devices and the diverse IoT ecosystem. Some of the key challenges include:

- **Proliferation of Devices:** The vast number and diverse range of IoT devices pose challenges in implementing uniform security measures throughout the entire IoT ecosystem. Each device may possess distinct hardware, software, and communication protocols, necessitating customized security solutions for individual cases.
- **Limitations in available resources**: Numerous IoT devices have constrained computing power, memory, and energy resources. Balancing the implementation of robust security measures with maintaining efficiency and performance presents a significant challenge.
- **Lack of Standardization:** The absence of standardized security protocols across IoT devices makes it difficult to enforce consistent security practices and increases the risk of vulnerabilities.
- **The security of the supply chain**: IoT devices often entail intricate supply chains with components sourced from multiple vendors. Ensuring the security of each component within the supply chain can pose significant challenges.
- **Over-the-Air Updates:** Remote updating of IoT devices can prove challenging due to limited connectivity or the potential risk of disrupting critical operations. Failing to apply timely updates may leave devices susceptible to known exploits.
- **Regulatory Compliance:** IoT devices may need to comply with various data protection and privacy regulations, adding complexity to IoT cybersecurity.
- **Lack of Security Awareness:** Certain IoT users might lack awareness of potential security risks or overlook basic security measures, rendering them susceptible to attacks.

Tackling these challenges necessitates a comprehensive and collaborative approach involving manufacturers, consumers, policymakers, and cybersecurity experts. Implementing robust authentication, encryption, regular updates, and secure communication protocols are critical steps to enhance IoT security and guarantee the secure and reliable operation of interconnected systems.

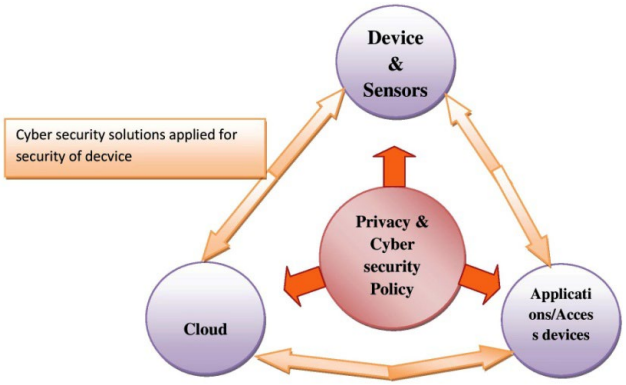

Figure 4: IoT cyber security & privacy.

VII. SOLVING THE SECURITY CHALLANGES:

To bolster IoT (Internet of Things) cybersecurity, a comprehensive approach encompassing technical, organizational, and policy measures is vital. Here are some key solutions to enhance IoT cybersecurity:

A. **Robust Authentication:** Enforce the implementation of robust authentication mechanisms, such as multi-factor authentication, to guarantee that only authorized users can access and manage IoT devices and networks.

B. **Data Encryption:** Employ end-to-end encryption for data transmitted between IoT devices and their associated servers to safeguard sensitive information from interception and unauthorized access.

C. **Regular Updates and Patch Management:** To safeguard against potential vulnerabilities and known exploits, it is essential to ensure that IoT devices receive regular updates and security patches in a timely manner.

D. **Ensuring the use of secure communication protocols:** Employ secure communication protocols, such as HTTPS, TLS, and IPsec, to safeguard data exchanged between IoT devices and servers effectively.

E. **Device Identity Management:** Establish a secure system for managing the identity and credentials of IoT devices to prevent unauthorized device impersonation.

F. **Hardware-Based Security:** Incorporate hardware-based security features, such as secure elements and trusted platform modules (TPMs), to enhance the integrity and authenticity of IoT devices.

G. **Secure Development Lifecycle:** Follow secure development practices, including security testing and code reviews, to build IoT devices with robust security from the outset.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 06, ISSN No. 2455-2143, Pages 48-55
Published Online October 2023 in IJEAST (http://www.ijeast.com)

H. **IoT Security Standards and Best Practices:** Adopt industry-wide security standards and best practices for IoT devices, fostering consistency and interoperability across the IoT ecosystem.
I. **Network Segmentation**: Deploy network segmentation to segregate IoT devices from critical systems, thereby minimizes the potential consequences of a security breach.
J. **Real-Time Threat Detection:** Employ advanced threat detection and intrusion detection systems (IDS) to identify suspicious activities and potential cyber threats in real-time.
K. **Data Privacy and Consent Management:** Establish well-defined data privacy policies and seek user consent for data collection and usage to safeguard users' privacy rights effectively.
L. **Secure Supply Chain Management:** Verify the security of IoT device components and ensure a secure supply chain to prevent the introduction of compromised hardware or software.
M. **Enhancing Security Awareness through Training Initiatives:** Enhance IoT Security Awareness: Users, Manufacturers, Employees
N. **Cooperation and Knowledge Exchange:** Promote cooperation among industry stakeholders, cybersecurity researchers, and policymakers to exchange threat intelligence and best practices.
O. **Regulatory Compliance:** Ensuring Legal and Ethical Cybersecurity Standards for IoT Devices: Complying with Data Protection and Privacy Regulations
P. **Regulatory Compliance:** Promote Legally and Ethically Compliant IoT Cybersecurity: Adhere to Data Protection Regulations.
Q. **Next-Generation Antivirus software (NGAV) represents the future of antivirus solutions:** Next-Generation Antivirus software (NGAV) has the capability to detect threats such as malware, even when they do not match known patterns or signatures.

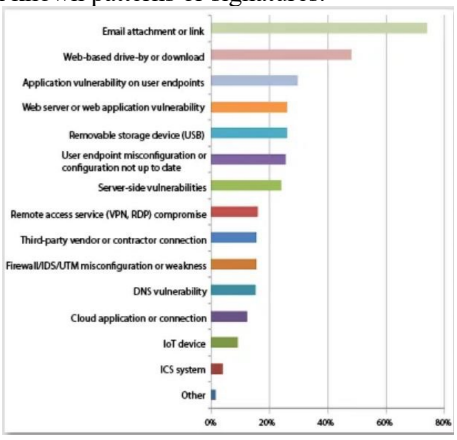

Figure 5: **Key security measures for safeguarding the IoT: Sourced from the SANS Institute.**

By adopting these solutions and incorporating cybersecurity as an integral part of IoT device development, deployment, and management, we can build a more secure and resilient IoT ecosystem, enhancing the safety and trustworthiness of interconnected smart devices.

VIII. FUTURE DIRECTIONS IN IOT CYBERSECURITY:

To address the growing concerns and challenges in IoT cybersecurity, there is a need for a comprehensive roadmap that outlines future directions in this domain. This roadmap should include the following key components:

A. **Increased collaboration and coordination:** Future directions in IoT cybersecurity should involve increased collaboration and coordination among various stakeholders, including governments, industry, academia, and cybersecurity experts.

B. **Development of standardized cybersecurity frameworks:** The future of IoT cybersecurity hinges on two crucial elements: standardized frameworks and the integration of artificial intelligence (AI) and machine learning (ML) technologies (Khanam, 2023). Standardized frameworks provide essential guidelines and best practices for securing IoT systems, covering authentication, encryption, access control, and device identity management. On the other hand, AI and ML integration offer enhanced cyber threat detection and prevention capabilities by continuously analyzing and learning from the vast data generated by IoT devices. Together, these advancements pave the way for a more secure and resilient IoT ecosystem.

C. **Continuous monitoring and threat intelligence:** Future directions in IoT cybersecurity should focus on the continuous monitoring of IoT systems and the collection of real-time threat intelligence. This will enable organizations to proactively detect and respond to cyber threats in a timely manner, minimizing the potential impact on IoT systems and networks.

IX. CONCLUSION

In summary, addressing IoT cybersecurity requires a multi-faceted approach involving strong authentication, encryption, regular updates, secure communication protocols, and hardware-based security. It also involves following secure development practices, adopting IoT security standards, and encouraging collaboration and information sharing. Looking ahead, the future of IoT cybersecurity will involve leveraging technologies like AI, blockchain, and quantum-safe cryptography. Implementing zero trust architecture, securing 5G networks, and focusing on user awareness and education will be crucial. Continuous vulnerability management, enhanced IoT device lifecycle management, and edge computing security are also part of the future direction.

Emphasizing simplicity and reducing complexity will be essential in ensuring a safer and resilient IoT ecosystem.

X. REFERENCE

[1]. Khanam, R... (2023, February 28). Review of Threats in IoT Systems: Challenges and Solutions. https://scite.ai/reorts/10.22214/ijraset.2023.49016

[2]. Tawalbeh, Loai & Muheidat, Fadi & Tawalbeh, Mais & Quwaider, Muhannad. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences. 10. 4102. 10.3390/app10124102.

[3]. Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.

[4]. Presser M, Krco Sa. IOT-I: Internet of Things Initiative: Public Deliverables – D2.1: Initial report on IoT applications of strategic interest 2010

[5]. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks 2010; 54(15):2787 – 2805, doi: 10.1016/j.comnet.2010.05.010.

[6]. 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.

[7]. Khvoynitskaya, S. The History and Future of the Internet of Things. 2020. Available online: https://www.itransition.com/: https://www.itransition.com/blog/iot-history (accessed on 25 March 2020)

[8]. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. **2018**, 78, 544–546. [Google Scholar] [CrossRef]

[9]. Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. **2020**, 10, 2088–8708. [Google Scholar]

[10]. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. IEEE Commun. Surv. Tutor. **2018**, 21, 1636–1675. [Google Scholar] [CrossRef]

[11]. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. **2018**, 25, 53–59. [Google Scholar] [CrossRef]

[12]. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30. [Google Scholar]

[13]. Izzat, A.; Chuck, E.; Lo'ai, T. The NICE Cyber Security Framework, Cyber Security Management; Springer: Basel, Switzerland, 2020; ISBN 978-3-030-41987-5. [Google Scholar]

[14]. Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. J. Inf. Secur. **2020**, 11. [Google Scholar] [CrossRef][Green Version]

[15]. Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406686 (accessed on 4 April 2020).

[16]. Tawalbeh, M.; Quwaider, M.; Tawalbeh, L.A. Authorization Model for IoT Healthcare Systems: Case Study. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 337–342. [Google Scholar] [CrossRef]

[17]. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. **2018**, 74, 340–354. [Google Scholar] [CrossRef]

[18]. Singh, J.; Thomas, F.J.-M.; Pasquier, J.B.; Ko, H.; Eyers, D.M. Twenty security considerations for cloud-supported Internet of Things. IEEE Internet Things J. **2016**, 3, 269–284. [Google Scholar] [CrossRef][Green Version]

[19]. The HIPAA Privacy Rule. Available online: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (accessed on 19 October 2019).

[20]. Thierer, A.D. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 2015.

[21]. Available online: http://jolt.richmond.edu/v21i2/article6.pdf (accessed on 6 March 2020).

[22]. Available online: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html (accessed on 17 March 2020).

[23]. L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[24]. Mahmoud, Rwan & Yousuf, Tasneem & Aloul, Fadi & Zualkernan, Imran. (2015). Internet of things (IoT)

security: Current status, challenges and prospective measures. 336-341. 10.1109/ICITST.2015.7412116

[25]. Sethi, P.; Sarangi, S. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. **2017**, 1–25. [Google Scholar] [CrossRef][Green Version]

[26]. Liyanage, M.; Braeken, A.; Kumar, P.; Ylianttila, M. IoT Security: Advances in Authentication; John Wiley & Sons: West Sussex, UK, 2020. [Google Scholar]

[27]. Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–175. [Google Scholar]

[28]. Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406686 (accessed on 4 April 2020).

[29]. W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. doi:10.1145/1062689.1062697. URL http://doi.acm.org/10.1145/1062689.1062697

[30]. Atlam, H.F., Attiya, G., El-Fishawy, N.: Comparative study on CBIR based on color feature. Int. J. Comput. Appl. 78(16), 975–8887 (2013)

[31]. Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D.: Twenty security considerations for cloud-supported Internet of things. IEEE Internet Things J. 3(3), 269–284 (2016)

[32]. Atlam, H.F., Alenezi, A., Walters, R., Wills, G.B.: An overview of risk estimation techniques in risk-based access control for the Internet of things. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), pp. 254–260 (2017)

[33]. M. Brachmann, O. Garcia-Morchon, S.-L. Keoh, S. S. Kumar, Security considerations around end-to-end security in the ip-based Internet of things, in: 2012 Workshop on Smart Object Security, in conjunction with IETF83, 2012, pp. 1–3.

[34]. M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepy smart object networks, in: 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 964–972. doi:10.1109/LCNW.2012.6424089.

[35]. M. Brachmann, S. L. Keoh, O. G. Morchon, S. S. Kumar, End-to-end transport security in the ip-based Internet of things, in: 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–5. doi:10.1109/ICCCN.2012.6289292.