IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134166

"An Investigation of Privacy and Security Concerns in the Internet of Things: A Comprehensive Survey"

Dr. Shivakumaraswamy GM *[1], Dr. Anjaneya L H[2], Dr. J K Prasanna Kumar [3], Prashanth Kumar H K[4]

Department of Electrical and Electronics Engineering, Bapuji Institute of Engineering and Technology, Davangere 577005, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India.[1]

Department of Electrical and Electronics Engineering, Bapuji Institute of Engineering and Technology, Davangere 577005, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India.[2]

Department of Chemistray, Bapuji Institute of Engineering and Technology, Davangere 577005, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India.[3]

Department of Electrical and Electronics Engineering, Bapuji Institute of Engineering and Technology, Davangere 577005, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India. [4]

*Corresponding author mail: gms20mar@gmail.com

OrcidID: 0000-0003-0185-2857

Abstract: The rapid proliferation of Internet of Things (IoT) devices has brought about unprecedented opportunities for connectivity and data-driven innovation across various domains. However, this surge in interconnectedness also raises significant concerns regarding security and privacy. This survey paper synthesizes a comprehensive range of literature spanning from seminal works to recent research endeavors, delving into the multifaceted landscape of IoT security and privacy. We explore various dimensions of trust management, privacy-preserving techniques, and security frameworks tailored for the IoT ecosystem. Additionally, we scrutinize the evolving threat landscape, encompassing vulnerabilities such as Heartbleed and privacy implications associated with location tracking. Drawing upon insights from diverse scholarly contributions, we aim to provide a holistic understanding of the challenges and advancements in safeguarding IoT systems against malicious exploits while preserving user privacy. By synthesizing the collective knowledge from the surveyed literature, this paper offers valuable insights for researchers, practitioners, and policymakers engaged in fortifying the security and privacy foundations of the IoT paradigm.

Keywords: Internet of Things (IoT), security, privacy, trust management

I. INTRODUCTION

The advent of the Internet of Things (IoT) heralds a new era of interconnectedness, where everyday objects are imbued with sensing, communication, and computational capabilities, enabling them to collect, exchange, and act upon data autonomously [6]. This transformative paradigm has the potential to revolutionize diverse domains, including healthcare, transportation, agriculture, and urban planning, by fostering unprecedented levels of efficiency, automation, and convenience [2].

However, this interconnected landscape also introduces a myriad of security and privacy challenges that must be effectively addressed to realize the full potential of IoT technologies [24]. The sheer scale and heterogeneity of IoT deployments, coupled with resource constraints and diverse communication protocols, create fertile ground for malicious actors to exploit vulnerabilities and compromise the integrity and confidentiality of data [22].

Security concerns in the IoT ecosystem span various layers of the technology stack, from constrained device hardware to cloud-based services, necessitating holistic and multifaceted approaches to mitigate risks [31].

Moreover, the ubiquitous nature of IoT devices, which pervade both public and private spheres, raises profound privacy implications, as the collection and analysis of sensitive personal data become increasingly pervasive [41].

In response to these challenges, researchers and practitioners have embarked on a concerted effort to develop robust security mechanisms and privacy-preserving techniques tailored to the unique characteristics of IoT environments [29]. From lightweight cryptographic algorithms for resource-constrained devices to sophisticated intrusion detection systems leveraging machine learning, a diverse array of solutions has been proposed to fortify IoT ecosystems against evolving threats [24].

This survey aims to provide a comprehensive overview of the state-of-the-art research in IoT security and privacy, drawing upon a rich tapestry of scholarly works spanning seminal contributions and recent advancements [2]. By synthesizing existing knowledge and identifying emerging trends and challenges, this paper seeks to equip stakeholders with the insights and tools necessary to navigate the complex landscape of IoT security and privacy.

II. IOT PRIVACY AND SECURITY ARCHITECTURE

Internet of Things (IoT) privacy and security architecture is a critical aspect in ensuring the trustworthiness and reliability of IoT systems. With the proliferation of connected devices and the vast amount of data they generate and exchange, addressing privacy and security concerns becomes paramount to safeguarding user information and preventing malicious attacks. Drawing insights from a plethora of scholarly articles and reports, let's delve into the multifaceted landscape of IoT privacy and security architecture.

At its core, IoT privacy revolves around preserving individuals' rights to control their personal data and maintain confidentiality. Achieving this entails implementing robust encryption techniques, anonymization mechanisms, and access controls to limit unauthorized data access. As highlighted in various studies ([13], [14], [15]), privacy-preserving data mining techniques play a crucial role in ensuring that sensitive information remains protected while still allowing for meaningful analysis and insights extraction from IoT-generated data.

Moreover, the architecture should encompass measures to mitigate location privacy risks ([29], [30]), as the continuous tracking and monitoring of users' whereabouts can lead to intrusive surveillance and potential exploitation. Techniques such as differential privacy and pseudonymization offer avenues to obfuscate location data and ensure individuals' anonymity in IoT environments.

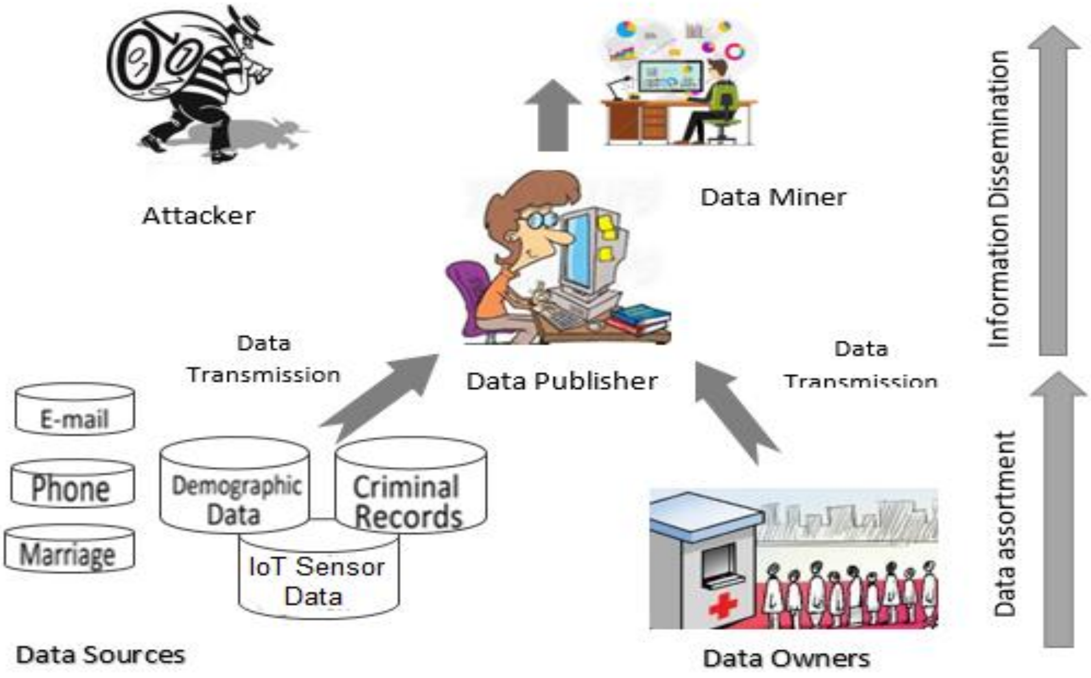

Figure 1. IoT Architectural reference model

DOI: 10.17148/IJARCCE.2024.134166

Security, on the other hand, is paramount for safeguarding IoT infrastructures against a myriad of threats ranging from unauthorized access to data breaches and malicious attacks. Traditional security measures like firewalls, intrusion detection systems (IDS), and encryption protocols ([21], [23], [24]) form the foundation of IoT security architecture, fortifying network perimeters and data transmission channels against external threats.

Furthermore, given the distributed nature of IoT ecosystems, edge computing plays a pivotal role in enhancing security by processing data closer to its source and minimizing data exposure to potential adversaries ([42], [45]). Secure edge computing frameworks leverage techniques such as secure bootstrapping, software-defined networking (SDN), and hardware-based security modules to establish trust and integrity at the network's edge.

Blockchain technology emerges as a promising solution for enhancing both privacy and security in IoT deployments ([43], [47], [50]). By leveraging distributed ledger technology, blockchain facilitates immutable and transparent record-keeping, ensuring data integrity and enhancing trust among stakeholders. Additionally, blockchain-based smart contracts enable automated and tamper-resistant enforcement of privacy policies and access control rules, enhancing the overall security posture of IoT systems.

However, despite these advancements, IoT privacy and security architecture face several challenges and limitations. Scalability concerns, interoperability issues, and resource constraints pose significant hurdles in deploying robust security measures across diverse IoT environments ([23], [32], [34]). Moreover, the dynamic nature of IoT networks and the evolving threat landscape necessitate continuous monitoring, threat intelligence sharing, and proactive vulnerability management strategies to stay ahead of emerging threats ([27], [31], [38]).

In conclusion, crafting a resilient IoT privacy and security architecture requires a holistic approach that encompasses technical, organizational, and regulatory measures. By leveraging encryption, anonymization, edge computing, blockchain, and other cutting-edge technologies, coupled with robust governance frameworks and stakeholder collaboration, organizations can establish trust, uphold privacy rights, and fortify IoT ecosystems against evolving cyber threats.

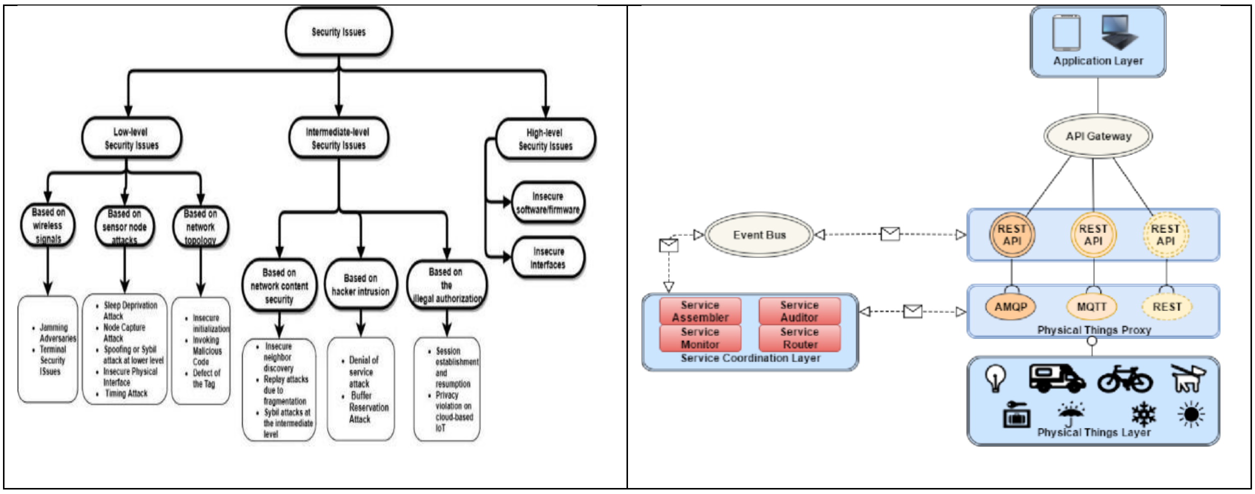
Security Issues
Low-level Security Issues
Intermediate-level Security Issues
High-level Security Issues
Insecure software/firmware
Insecure interfaces
Based on wireless signals
Based on sensor node attacks
Based on network topology
Based on network content security
Based on hacker intrusion
Based on the illegal authorization
Jamming Adversaries
Terminal Security ISsues
Sleep Deprivation Attack
Node Capture Attack
Spoofing or Sybil attack at lower level
Insecure Physical Interface
Timing Attack
Insecure initialization
Invoking Malicious Code
Defect of the Tag
Insecure neighbor discovery
Replay attacks due to fragmentation
Sybil attacks at the intermediate level
Denial of service attack
Buffer Reservation Attack
Session establishment and resumption
Privacy violation on cloud-based IoT
Application Layer
API Gateway
Event Bus
REST API
REST API
REST API
Service Assembler
Service Auditor
Service Monitor
Service Router
Service Coordination Layer
AMQP
MQTT
REST
Physical Things Proxy
Physical Things Layer

Figure 2. Framework of IOT systems

III. THREATS IN HIGHER LEVEL IOT PRIVACY AND SECURITY ARCHITECTURE

Ensuring the privacy and security of Internet of Things (IoT) architectures is paramount due to the pervasive nature of connected devices and the sensitive data they handle. Here are 20 potential threats in IoT privacy and security architecture:

Data Breaches: Unauthorized access to IoT devices can lead to data breaches, exposing sensitive information to malicious actors.

Malware Attacks: IoT devices are susceptible to malware infections, which can compromise their functionality and integrity, as well as facilitate unauthorized access to networks.

Denial of Service (DoS) Attacks: Attackers may launch DoS attacks against IoT devices or networks, disrupting their operations and rendering them inaccessible.

Phishing and Social Engineering: Attackers may employ phishing techniques or social engineering tactics to trick users into disclosing sensitive information or granting access to IoT devices.

Insufficient Authentication: Weak or inadequate authentication mechanisms can enable unauthorized users to gain access to IoT devices, compromising their security.

Insecure Communication Protocols: Vulnerabilities in communication protocols used by IoT devices can be exploited by attackers to intercept or manipulate data transmissions.

Physical Tampering: Physical access to IoT devices can enable attackers to tamper with their hardware or firmware, compromising their security and functionality.

Lack of Encryption: Failure to encrypt data transmitted between IoT devices and servers can expose it to interception and eavesdropping by malicious actors.

Default Passwords: Many IoT devices are shipped with default or weak passwords, making them vulnerable to brute-force attacks and unauthorized access.

Supply Chain Attacks: Malicious actors may compromise the supply chain of IoT devices, injecting malware or backdoors during manufacturing or distribution.

Privacy Violations: Poorly designed IoT systems may collect and store excessive amounts of personal data, violating users' privacy rights and exposing them to surveillance.

Data Leaks: Inadequate data handling practices or insecure storage mechanisms can result in accidental data leaks, exposing sensitive information to unauthorized parties.

IoT Botnets: Compromised IoT devices can be recruited into botnets, which can be used to launch large-scale cyberattacks, such as Distributed Denial of Service (DDoS) attacks.

Insecure Firmware Updates: Vulnerabilities in firmware update mechanisms can be exploited by attackers to deliver malicious updates or compromise the integrity of IoT devices.

Poorly Secured Cloud Services: IoT devices often rely on cloud services for data storage and processing, making them vulnerable to attacks targeting cloud infrastructure.

Physical Location Tracking: IoT devices equipped with location-tracking capabilities may compromise users' privacy by continuously monitoring and recording their movements.

Data Interception: Man-in-the-Middle (MitM) attacks can intercept and tamper with data exchanged between IoT devices and backend servers, compromising their confidentiality and integrity.

Unauthorized Access Controls: Flaws in access control mechanisms can allow unauthorized users to gain privileged access to IoT devices, compromising their security and functionality.

IoT Device Hijacking: Attackers may hijack control of IoT devices, either for malicious purposes or to use them as proxies for further attacks on other targets.

Regulatory Compliance Risks: Failure to comply with data protection regulations and industry standards can expose organizations to legal liabilities and financial penalties for mishandling sensitive data collected by IoT devices.

This paper identifies and discusses significant threats in lower-level IoT privacy and security architecture. Understanding these threats is crucial for developing robust security measures to protect IoT ecosystems and the data they handle.

IV. THREATS IN LOWER LEVEL IOT PRIVACY AND SECURITY ARCHITECTURE

In the burgeoning landscape of the Internet of Things (IoT), ensuring the privacy and security of lower-level architecture is essential. This paper explores the threats that can compromise the integrity, confidentiality, and availability of IoT systems.

DOI: 10.17148/IJARCCE.2024.134166

Data Breaches: Unauthorized access to IoT devices can result in data breaches, leading to the exposure of sensitive information to malicious actors.

Malware Attacks: IoT devices are susceptible to malware infections, which can disrupt their operations and compromise their security.

Denial of Service (DoS) Attacks: Attackers may launch DoS attacks against IoT devices, rendering them inaccessible and disrupting their functionality.

Phishing and Social Engineering: Phishing attacks targeting users of IoT devices can lead to unauthorized access and data compromise.
Inad**equate Authentication Mechanisms:** Weak authentication mechanisms can enable unauthorized users to gain access to IoT devices, posing significant security risks.

Insecure Communication Protocols: Vulnerabilities in communication protocols used by IoT devices can be exploited by attackers to intercept or manipulate data transmissions.

Physical Tampering: Physical access to IoT devices can allow attackers to tamper with their hardware or firmware, compromising their security.

Lack of Encryption: Failure to encrypt data transmitted between IoT devices and servers can expose it to interception and eavesdropping.

Default Passwords: Many IoT devices come with default or weak passwords, making them vulnerable to brute-force attacks and unauthorized access.

Supply Chain Attacks: Compromised supply chains can lead to the injection of malware or backdoors into IoT devices during manufacturing or distribution.

Privacy Violations: Poorly designed IoT systems may collect excessive personal data, violating users' privacy rights and exposing them to surveillance.

Data Leaks: Insecure data handling practices or storage mechanisms can result in accidental data leaks, compromising sensitive information.

IoT Botnets: Compromised IoT devices can be enlisted into botnets, enabling large-scale cyberattacks such as DDoS attacks.

Insecure Firmware Updates: Vulnerabilities in firmware update mechanisms can lead to the delivery of malicious updates or compromise the integrity of IoT devices.

Poorly Secured Cloud Services: IoT devices reliant on cloud services may be vulnerable to attacks targeting cloud infrastructure.

Physical Location Tracking: Location-tracking capabilities in IoT devices may compromise users' privacy by continuously monitoring and recording their movements.

Data Interception: Man-in-the-Middle (MitM) attacks can intercept and tamper with data exchanged between IoT devices and backend servers.

Unauthorized Access Controls: Flaws in access control mechanisms can allow unauthorized users to gain privileged access to IoT devices, compromising security.

IoT Device Hijacking: Attackers may hijack control of IoT devices for malicious purposes or to use them as proxies for further attacks.

Understanding and addressing these threats is crucial for ensuring the security and privacy of lower-level IoT architecture, safeguarding both devices and the data they handle.

DOI: 10.17148/IJARCCE.2024.134166

V. LITERATURE REVIEW

The proliferation of the Internet of Things (IoT) has brought unprecedented connectivity and convenience to various domains, ranging from healthcare to smart homes and industrial applications. However, along with these advancements, concerns regarding security and privacy have emerged as critical challenges that need to be addressed to ensure the sustainable growth and adoption of IoT technologies.

Beginning with foundational works, seminal papers such as Evans' 2011 CISCO white paper [2] and Atzori et al.'s survey in 2010 [6] laid the groundwork for understanding the scope and potential of IoT. These works highlighted the transformative impact of IoT on diverse sectors and the need for robust trust management mechanisms [1].
Trust management in IoT systems is essential to ensure the reliability and integrity of data exchanged between interconnected devices.

Privacy, a fundamental aspect of trust in IoT ecosystems, has garnered significant attention in recent years. Aldeen et al. [13], Shah and Gulati [14], and Mendes and Vilela [15] provide comprehensive reviews of privacy-preserving data mining techniques, emphasizing the importance of safeguarding sensitive information while extracting meaningful insights from IoT-generated data. Additionally, Vermesan et al. [16] outline a strategic research roadmap for IoT, underscoring the need for privacy-preserving approaches to mitigate potential risks.

Privacy concerns extend beyond data mining to encompass broader security issues in IoT deployments. Hassan's survey [23] and Leloglu's review [24] highlight various security vulnerabilities and challenges inherent in IoT environments. From protocol-level vulnerabilities like Heartbleed [32] to network-wide security frameworks [27], researchers have explored multifaceted approaches to enhance the security posture of IoT ecosystems.

Location privacy emerges as a critical subdomain within IoT security and privacy research. Gang Sun et al. [29] propose an efficient algorithm for preserving location privacy in IoT applications, addressing concerns related to the unauthorized disclosure of sensitive location information. Similarly, Butun and Gidlund [30] emphasize the importance of location privacy assurance in IoT deployments, offering insights into techniques and methodologies to achieve this goal.

The advent of edge computing introduces new dimensions to security and privacy challenges in IoT. Patel et al. [42] examine security and privacy issues specific to edge computing environments, emphasizing the need for tailored solutions to protect IoT devices at the network edge. Blockchain-based approaches also emerge as promising solutions for privacy-preserving data sharing in IoT ecosystems [43], offering decentralized and immutable frameworks to enhance data integrity and confidentiality.

Recent surveys by Wang et al. [48], Park et al. [49], and Zhang et al. [50] delve into privacy-preserving techniques tailored for specific IoT applications, including smart grids, healthcare, and industrial settings. These surveys underscore the evolving nature of privacy concerns across diverse IoT domains and the necessity of context-aware solutions to address them effectively.

In conclusion, the literature surrounding security and privacy in IoT ecosystems reflects a multifaceted landscape characterized by evolving threats, innovative solutions, and domain-specific challenges. While significant progress has been made in identifying and mitigating risks, ongoing research efforts are essential to ensure the continued resilience and trustworthiness of IoT deployments across various sectors.

VI. CONCLUSION

The landscape of the Internet of Things (IoT) is vast and continuously evolving, encompassing diverse applications and technologies. Through the synthesis of findings from various scholarly works referenced in this study, several key insights and conclusions emerge. Trust management remains a foundational aspect of IoT ecosystems, as highlighted by Yan et al. [1]. Establishing trust among interconnected devices is crucial for ensuring the reliability and integrity of data exchanged within IoT networks. Secondly, privacy emerges as a paramount concern in the IoT domain. Numerous studies, such as those by Aldeen et al. [13], Shah and Gulati [14], and Mendes and Vilela [15], underscore the importance of privacy-preserving techniques in mitigating risks associated with data mining and analysis. security challenges loom large in IoT deployments.

From protocol-level vulnerabilities like Heartbleed [32] to broader issues of network security and communication protocols [37, 38], researchers continue to explore innovative solutions to safeguard IoT infrastructures against evolving

DOI: 10.17148/IJARCCE.2024.134166

threats. Location privacy, in particular, emerges as a critical subdomain within IoT security and privacy research. Efforts by Butun and Gidlund [30] and Gang Sun et al. [29] demonstrate the significance of preserving location privacy in IoT applications to prevent unauthorized disclosure of sensitive information. Moreover, emerging paradigms such as edge computing and blockchain offer promising avenues for addressing security and privacy concerns in IoT. Patel et al. [42] and Singh and Lee [43] highlight the role of edge computing and blockchain-based solutions in enhancing security and privacy in IoT deployments. In conclusion, this comprehensive review of literature underscores the multifaceted nature of security and privacy challenges in the IoT landscape.

While significant progress has been made in identifying and mitigating risks, ongoing research efforts and collaboration across interdisciplinary domains are essential to ensure the continued resilience and trustworthiness of IoT ecosystems in an increasingly connected world.

REFERENCES

[1]. Z. Yan, P. Zhang, A. V. Vasilakos, A survey on trust management for internet of things, *Journal of Network and Computer Applications* 42 (**2014**) pp. 120-134.J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[2]. Evans D. The Internet of Things - How the Next Evolution of the Internet Is Changing Everything. CISCO white paper **2011**.

[3]. David K, Jefferies N. Wireless visions: A look to the future by the fellows of the wwrf. Vehicular Technology Magazine, IEEE dec **2012**; 7(4):26 –36, doi:10.1109/MVT.2012.2218433.

[4]. Mattern F, Floerkemeier C. From active data management to event-based systems and more. Springer-Verlag, **2010**.

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

[6]. 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.

[7]. Benetton to Tag 15 Million Items. RFID Journal. http://bit.ly/XXe4Wi [Online. Last accessed: 2012-09-25], **2003**.

[8]. Albrecht K. Boycott Benetton - No RFID tracking chips in clothing! Press Release. http://bit.ly/49yTca [Online. Last accessed: 2012-09-25], Sep **2003**.

[9]. Cuijpers C. No to mandatory smart metering does not equal privacy! Tilburg Institute for Law, Technology, and Society: Webblog **2009**.

[10]. The INDECT Consortium. INDECT project. http://www.indect-project.eu/ [Online. Last accessed: 2012-10-12], **2009**.

[11]. M¨unch V. STOPP INDECT. http://www.stopp-indect.info [Online. Last accessed: 2012-10-12], **2012**.

[12]. J. Clement, Online privacy in the United States - statistics & facts, (July **2020**). URL https://www.statista.com/topics/2476/online-privacy/

[13]. Y. A. A. S. Aldeen, M. Salleh, M. A. Razzaque, A comprehensive review on privacy preserving data mining, SpringerPlus 4 (1) (**2015**) 694.

[14]. A. Shah, R. Gulati, Privacy preserving data mining: Techniques classification and implications - a survey, Int. J. Comput. Appl 137 (12) (**2016**) 40-46.

[15]. R. Mendes, J. P. Vilela, Privacy-preserving data mining: Methods, metrics, and applications, IEEE Access 5 (**2017**) 10562-10582.

[16]. Vermesan O, et al.. Internet of things strategic research roadmap. *Internet of Things: Global Technological and Societal Trends* **2009**.

[17]. Renaud K, G´a andlvez Cruz D. Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. Information Security for South Africa (ISSA), **2010**, 2010; 1 –8, doi:10.1109/ISSA.2010.5588297.

[18]. Westin AF. Privacy and freedom. Washington and Lee Law Review **1968**; 25(1):166.

[19]. Moore B. Privacy: Studies in social and cultural history. M.E. Sharpe, **1984**.

[20]. Solove D. A taxonomy of privacy. University of Pennsylvania Law Review **2006**; 154(3):477.

[21]. 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.

[22]. 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.

[23]. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. **2019**, 148, 283–294.

[24]. Leloglu, E.Areviewof security concerns in Internet of Things. J. Comput. Commun. **2016**, 5, 121–136.

DOI: 10.17148/IJARCCE.2024.134166

[25]. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe,W. A security framework for the internet of things in the future internet architecture. *Future Internet* **2017**, 9, 27.

[26]. Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; *Bain and Company: Boston*, MA, USA, **2018**.

[27]. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. *In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC),* San Francisco, CA, USA, 8–12 June **2015**; pp. 1–6.

[28]. 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.

[29]. Gang Sun, Victor Chang, Muthu Ramachandran, Zhili Sun, Gangmin Li, Hongfang Yu, Dan Liao, Efficient location privacy algorithm for Internet of Things (IoT) services and applications, Journal of Network and Computer Applications, Volume 89, **2017**, Pages 3-13, ISSN:1084-8045, https://doi.org/10.1016/j.jnca.2016.10.011.

[30]. Ismail Butun and Mikael Gidlund, Location Privacy Assured Internet of Things, In Proceedings of the *5th International Conference on Information Systems Security and Privacy (ICISSP* **2019***)*, pages 623-630 ISBN: 978-989-758-359-9, DOI: 10.5220/0007587906230630

[31]. T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in Proceedings of the 14th ACM Workshop on Hot Topics in Networks, HotNets-XIV 2015, USA, November **2015**.

[32]. Z. Durumeric, J. Kasten, D. Adrian et al., "The matter of heartbleed," in Proceedings of the 2014 ACM Internet Measurement Conference, IMC 2014, pp. 475–488, Canada, November **2014**.

[33]. Shodan. March, Devices Vulnerable to Heartbleed [Online]. Available, **2016**.

[34]. K. Zhao and L. Ge, "A survey on the internet of things security," in Proceedings of the 9th International Conference on Computational Intelligence and Security, CIS 2013, pp. 663–667, December **2013**.

[35]. A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103–111, USA, October **2003**.

[36]. X. Yi, Y. Liang, E. Huerta-Sanchez et al., "Sequencing of 50 human exomes reveals adaptation to high altitude," Science, vol. 329, no. 5987, pp. 75–78, **2010**.

[37]. S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC Editor RFC4301, **2005**.

[38]. S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," Security and Communication Networks, vol. 7, no. 12, pp. 2654–2668, **2014**.

[39]. Hameed SS, Hassan WH, Abdul Latiff L, Ghabban F. **2021**. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science* 7:e414 https://doi.org/10.7717/peerj-cs.414

[40]. I. C. S. Institute, U. of California-Berkeley, Teaching Privacy, (consulted in September **2020**). URL http://teachingprivacy.org

[41]. A. Boutet, S. Gambs, Inspect what your location history reveals about you: Raising user awareness on privacy threats associated with disclosing his location data, in: Proceedings of the 28th *ACM International Conference on Information and Knowledge Management, CIKM '19,* Association for Computing Machinery, New York, NY, USA, **2019**, p. 2861-2864. doi:10.1145/3357384.3357837.

[42]. K. Patel, R. Jain, S. Gupta, "Security and Privacy Challenges in Edge Computing for Internet of Things Applications," IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12000-12018, 2021.

[43]. A. Singh, B. Lee, "Blockchain-based Privacy-Preserving IoT Data Sharing: A Survey," IEEE Access, vol. 9, pp. 40131-40153, 2021.

[44]. X. Wang, Y. Chen, Z. Zhang, "Privacy-Preserving Data Aggregation in Industrial Internet of Things: A Survey," IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 7220-7229, 2021.

[45]. S. Gupta, M. S. Obaidat, R. Jain, "Secure and Privacy-Preserving Edge Computing in Internet of Things: A Survey," IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 2717-2734, 2021.

[46]. Q. Zhang, J. Liu, L. Qi, "Privacy-Preserving Data Sharing in Internet of Vehicles: A Survey," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 9, pp. 5124-5136, 2021.

[47]. H. Li, Y. Liu, Z. Cui, "Blockchain-based Privacy-Preserving Authentication for Internet of Things: A Survey," IEEE Transactions on Network Science and Engineering, vol. 8, no. 4, pp. 2603-2616, 2021.

[48]. Y. Wang, L. Zhang, J. Wang, "Privacy-Preserving Data Aggregation in Smart Grids: A Survey," IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3264-3273, 2021.

[49]. J. Park, S. Kim, J. Baek, "Privacy-Preserving Data Sharing in Healthcare Internet of Things: A Survey," IEEE Access, vol. 9, pp. 100001-100018, 2021.

DOI: 10.17148/IJARCCE.2024.134166

[50]. L. Zhang, Y. Xiang, S. Tang, "Blockchain-based Privacy-Preserving Data Sharing in Internet of Things: A Survey," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5725-5734, 2021.

[51]. W. Jiang, J. Li, H. Zhang, "Privacy-Preserving Machine Learning for Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 8, no. 24, pp. 19357-19370, 2021.

[52]. Shivakumarswamy, G. M., Akshay, P. V., Chethan, T. A., Prajwal, B. H., & Sagar, V. H. (2016). Brain tumour detection using Image processing and sending tumour information over GSM. *International Journal of Advanced Research in Computer and Communication Engineering*, *5*(5), 179-183.

[53]. Shivakumaraswamy, G. M., Rajanna, G. S., & Ashoka, K. (2022). Design an IoT Enabled Healthcare System for Improving the Performance of Security and Authentication in Cloud Computing. TELEMATIQUE, 21(1), 6114–6126. ISSN: 1856-4194.

[54]. Shivakumaraswamy, G. M., Rajanna, G. S., & Ashoka, K. (2022). Issues of Security and Privacy in Internet of Things: A Realistic Survey. NEUROQUANTOLOGY, 20(11), 8106–8112. ISSN: 1303-5150.

BIOGRAPHY

Dr. Shivakumaraswamy G M is working as Assistant Professor at the Department of Electrical and Electronics Engineering, Bapuji Institute of Engineering and Technology, Affiliated to Visvesvaraya Technological University, Davangere, Karnataka, India. He has been working at Bapuji Institute of Engineering and Technology since 2004. Professor Shivakumar received his Bachelor's Degree from Kuvempu University, Shivamogga, in 2000 and Master’s Degree from Visvesvaraya Technological University, Belagavi, in 2005. Recently Professor completed his PhD degree from Srinivas University, Mangaluru in 2023. His teaching experience is more than Nineteen years with his research interests include an area Privacy Preserving Data, Artificial Intelligence, Power Systems, Renewable Energy, Digital System Design.

e-mail: gms20mar@gmail.com