iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 Issue: VI Month of publication: June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54519

Review of Effect of Internet of Things(IoT) in Cybercrime

Sanyam Agarwal[1], Veer Daksh Agarwal[2], Vipin Mittal[3], Ishaan Agarwal[4]
[1]*Department of Electronics & Communication Engineering, ACE College of Engineering & Management, Agra, India*
[2]*Department of Computer Science Engineering, Thapar Institute Of Engineering & Technology, Patiala, India*
[3]*Department of Electronics & Communication Engineering, IIMT university, Meerut, India…*
[4]*Department, of Computer Science Engineering, SRM institute of Science & Technology, Kattankulathur, Chennai, India*

Abstract: This review paper examines the impact of the Internet of Things (IoT) in cybercrime. With the rise of IoT devices, cyber-attacks have also increased immensely, leading to new security challenges. IoT devices frequently lack the security of traditional computers, leaving them open to hacking and other forms of online assaults. Attackers can use IoT devices as a way to gain access to networks or other devices, steal data, or launch attacks. This paper gives a broad review of the security issues IoT devices pose and how cybercriminals take advantage of them. It also discusses the measures that can be taken to secure IoT devices and protect against cyber-attacks.

The discussion of potential future study topics for examining how IoT is affecting cybercrime finishes the paper. Overall, this review paper highlights the importance of understanding the risks associated with IoT devices and implementing appropriate security measures to mitigate them.

Keywords: Internet of Things, Cybercrime, Security Challenges, Hacking, Data Privacy, Cyber Security, Cyber-attacks

I. INTRODUCTION

The Internet of Things (IoT)[47] enables seamless connection and device automation and has completely changed how we engage with technology.[14] However, as IoT devices become more prevalent in our residences, places of employment, and public areas causing an increased risk of cybercrime.[10][38]

The role of IoT in cybercrimes may be observed in the different ways that hackers can take advantage of flaws in IoT hardware to access confidential data, launch attacks, and jeopardize security and privacy.[40][41] Understanding the risks and difficulties related to IoT-based cybercrimes is crucial as the amount of connected devices rises, and exploring ways to mitigate them through proactive security measures and collaboration between different stakeholders.

II. TYPES OF CYBERCRIMES

There are different types of cybercrimes, including:

1) *Hacking:* To take an unauthorized access of a computer system or network to steal data or cause damage.
2) *Phishing:* The practice of tricking individuals or firms into disclosing sensitive information, including passwords or credit card data, through phony emails, websites, or different techniques.
3) *Malware:* It is the practice of breaking into or harming computer systems using malicious software like viruses, worms as well as Trojan horses.
4) *Denial-of-service (DoS) or Distributed Denial-of-Service (DDoS) Attacks***:** The widespread usage of computers to overwhelm a website or network, preventing legitimate users from accessing it, is called DoS.
5) *Identity Theft:* Theft of personal data for financial benefits, such as bank account information or Social Security numbers.[3]
6) *Cyber Bullying:* Using technology to harass, intimidate, or threaten someone online.
7) *Cyber Stalking:* Using technology to track or monitor someone without their consent.
8) *Ransomware:* The use of malicious software to encrypt files or systems, demanding payment in exchange for the decryption key.
9) *Intellectual Property Theft:* The theft of trade secrets, patents, or copyrighted material.
10) *Cyber Espionage:* Hacking and other techniques to steal classified or sensitive information from governments or businesses.[41]

Year	Data breaches and exposures (1)	Number of individuals impacted (millions)
2016	1099	2541.1
2017	1506	1825.4
2018	1175	2227.8
2019	1279	883.6
2020	1108	310.1
2021	1862	293.9
2022	1802	422,1

Fig1. Rise of Cybercrime

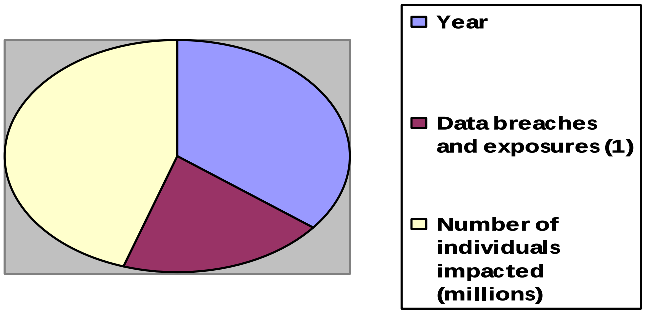


Fig2.Number of Data Breaches and Individuals Impacted 2016-2022

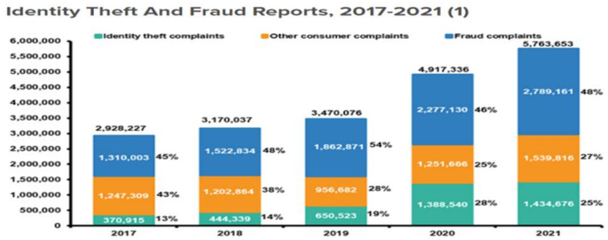


Fig3.Theft and Fraud data

III.TYPES OF CYBERCRIMES USING IOT

The Internet of Things (IoT) has introduced new kinds of cybercrimes. Some examples of cybercrimes with the help of IoT include:

1) *Botnets:* Hackers can take control of IoT devices, such as smart home devices or cameras, to create a network of compromised devices called a botnet. The botnet can then be used to launch attacks on websites or other networks.[34]
2) *IOT-based DDoS Attacks:* Distributed denial-of-service (DDoS) assaults on websites or other networks can be launched by hackers using hacked IoT devices, resulting in their crash or unavailability.[13]
3) *Data Theft:* IoT devices frequently gather and send private data, including financial and personal information. These data are susceptible to interception or theft by hackers due to faults in IoT networks or devices.
4) *Malware:* Malicious software can be installed on IoT devices, allowing hackers to access other network devices or steal data.
5) *Physical Damage:* IoT devices can be targeted to cause physical damage, such as hacking into smart home systems to control appliances or sabotaging industrial control systems.
6) *IOT-based Phishing Attacks:* Hackers can use compromised IoT devices to launch phishing attacks, which use fraudulent emails or websites to trick people into providing sensitive information.
7) *Ransomware Attacks:* Hackers can install ransomware on IoT devices, encrypting the data and demanding payment in exchange for the decryption key.[37]
8) *IOT-based Identity Theft:* Hackers can collect passwords and usernames from hacked IoT gadgets and use them to perform identity theft.

9) *Physical Attacks:* Crypto analysis, or the study of computer systems to uncover devices' and systems' hidden features using their execution characteristics, includes physical assaults.[4]
10) *Node Replication:* A preexisting node id is replicated to a network of devices with sensors in this attack. Due to node replication, packets may be improperly routed, incorrect sensor readings may be captured, or the network may become disconnected. As a result, a sensor network's functionality is compromised.[42]
11) *Selective Forwarding:* The nodes in a WSN forward messages to their intended recipient. In this attack, a rogue node sends packets arbitrarily. Some emails can just be deleted without being forwarded. The message is transmitted to different nodes after the packets coming from a select few nodes are modified. As a result, it is challenging to locate the attacker.
12) *Wormhole Attack:* It is a severe attack where packets are captured at one point on the network and then replayed at another. This process can be applied selectively.
13) *Sybil Attack:* When a system is taken over, and the hacker assumes many identities, this is known as a Sybil attack. In this type of cybercrime, an enemy may be able to be in many places at once during this strike. In this case, a single node in the network assumes numerous identities, which significantly reduces the efficiency of fault tolerance.[43]
14) *Sinkhole Attack:* In this kind of assault, a hacker hijacks a network node and draws all of the traffic from other nodes. The routing method is used to carry out this procedure, and additional nodes are drawn to it. As a result, being a component of the routing procedure, several attacks, such as selective packet forwarding, message modifications, and packet deletion, are possible.
15) *Service Attack Denial:* Legitimate users are prevented from accessing the services. Here, the attacker overwhelms the links of the victims with valid requests, breaking those linkages. As a result, all services are refused to authorized users.
16) *Eavesdropping:* In this type of attack, the intrusive party listens to the data while it is being sent across the two nodes via the network. Information is still being shared here, but privacy is being jeopardized. The invaders may utilize this information to harm the users.[32]

IOT ATTACKS	Device	High end-class, low end-class
	Location	Internal, external
	Access Level	Active, passive
	Information Damage Level	Interruption, eavesdropping, node replication, modification, fabrication, man-in-the-middle, replay
	Host Promise	User, hardware, software
	Strategy	Physical, logical
	Protocol-based	Disruption ,Deviation
	Layer-based	Perception, Network, Middleware, Application, Interface
	Major Attacks	DoS, Wormholes, Spoofed, alter or replayed routing information , Sybil[36]

Fig4. Classification of Security parameters & attack vectors

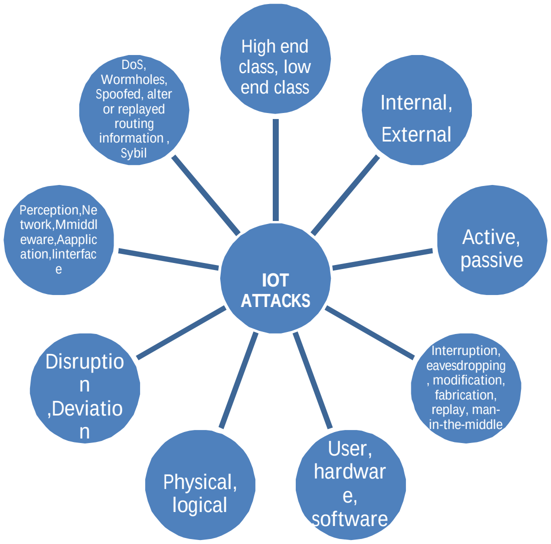
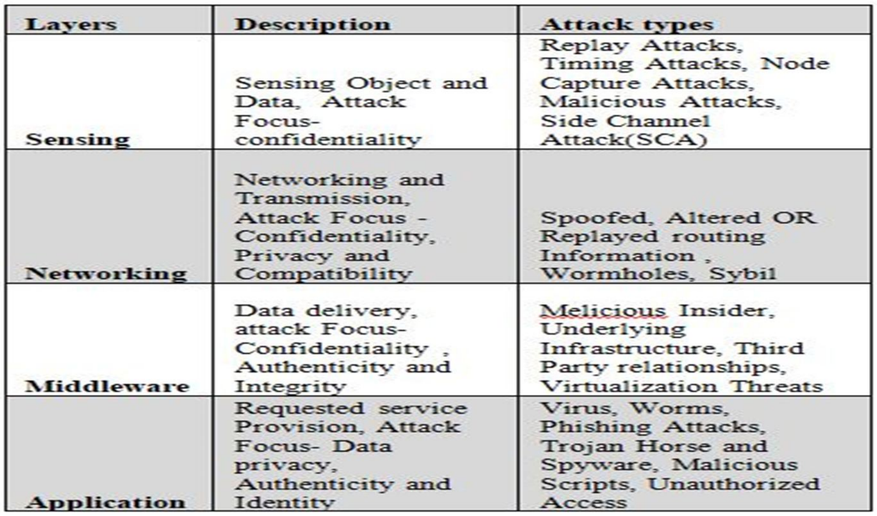

High end class, low end class
Internal, External
Active, passive
Interruption, eavesdropping, modification, fabrication, replay, man-in-the-middle
User, hardware, software
Physical, logical
Disruption ,Deviation
Perception,Network,Mmiddleware,Aapplication,Iinterface
DoS, Wormholes, Spoofed, alter or replayed routing information , Sybil
IOT ATTACKS

Fig5. IOT Attacks Vectors

IV.TYPICAL STRUCTURE AND MAJOR TYPE OF ATTACKS

The typical Network Structure of a digital network is as shown in the figure consisting of all the major sensing, network, middleware and application layer and also the type of most effective attacks in the network



Layers	Description	Attack types
Sensing	Sensing Object and Data, Attack Focus-confidentiality	Replay Attacks, Timing Attacks, Node Capture Attacks, Malicious Attacks, Side Channel Attack(SCA)
Networking	Networking and Transmission, Attack Focus - Confidentiality, Privacy and Compatibility	Spoofed, Altered OR Replayed routing Information , Wormholes, Sybil
Middleware	Data delivery, attack Focus-Confidentiality , Authenticity and Integrity	Melicious Insider, Underlying Infrastructure, Third Party relationships, Virtualization Threats
Application	Requested service Provision, Attack Focus- Data privacy, Authenticity and Identity	Virus, Worms, Phishing Attacks, Trojan Horse and Spyware, Malicious Scripts, Unauthorized Access

Fig 6 Security layer and associated attack types

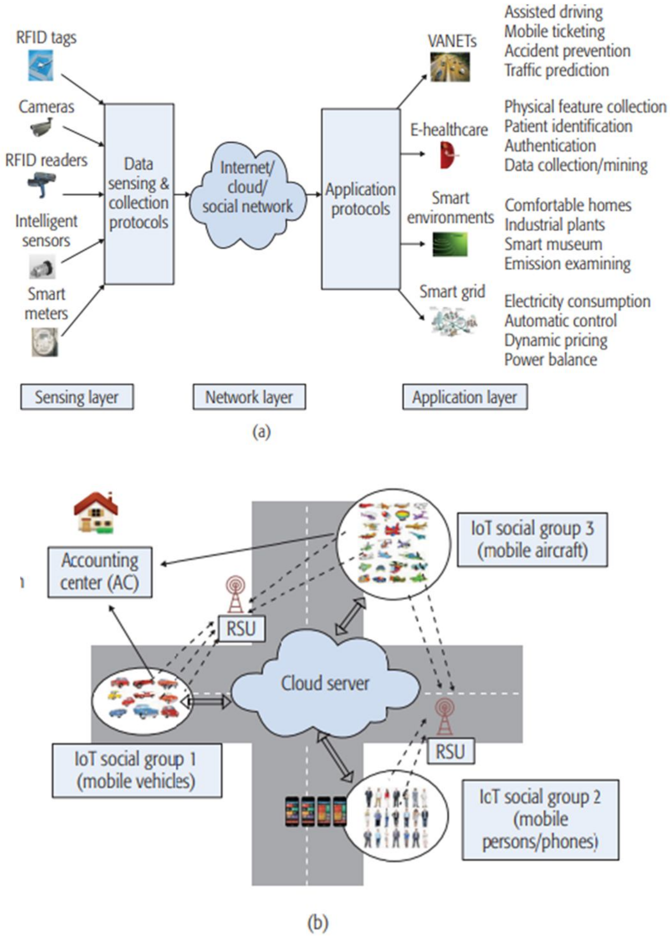


Fig7. Typical Infrastructure of a IOT network

V. INEFFICIENCY IN CURRENT SYSTEM

Current IoT systems are inefficient against cybercrime for several reasons:

1) *Lack of Security by Design:* Instead of security, simplicity and utility are the primary design considerations for many IoT devices. They frequently lack fundamental security components like encryption, verification, and accessibility control as a result, leaving them open to cyber-attacks.[21]
2) *Complexity:* IoT systems are complex and diverse, consisting of a wide range of devices, protocols, and technologies, which can make them difficult to secure and manage.[48]
3) *Limited Resources:* It can be difficult to apply security measures without compromising speed since many IoT devices have constrained computational resources, including memory and processing capacity.[44]
4) *Lack of Standardization:* There is currently no widely accepted standard for IoT security, which can lead to inconsistencies in security practices across different devices and vendors.[20]
5) *Rapidly Evolving Threats:* Cybercriminals are constantly developing new and sophisticated techniques to exploit vulnerabilities in IoT systems, making it difficult for security measures to keep pace.[23]
6) *Ineffective Patch And Updating Procedures:* A lot of IoT devices are not made to regularly update their software, making them susceptible to known security issues and attacks.[22]

Addressing these challenges will require a concerted effort from industry, government, and consumers to prioritize security by design, implement best practices for securing IOT devices, and collaborate on developing standards and regulations that promote IOT security.

VI. SECURITY MEASURES/RECOMMENDATIONS

IoT can be used to fight against cybercrimes in several ways:

1) *Device Security:* IoT devices can be designed with built-in security features such as encryption, authentication, and access control to protect against unauthorized access and hacking attempts.[19]
2) *Real-time Monitoring:* IoT devices can be used to monitor systems and detect suspicious activity in real time. For example, an IoT-based intrusion detection system can identify unauthorized access to a network and alert security personnel.[50]
3) *Big Data Analytics:* Large volumes of data are generated by IoT devices, which may be analyzed with machine learning, deep learning, and other analytical techniques to look for trends and abnormalities that can point to cyber-attacks.[24]
4) *Threat Intelligence:* IoT devices can collect threat intelligence from various sources such as dark web forums and social media to identify potential cyber threats.[34]
5) *Incident Response:* IoT devices can be used to automate incident response processes, such as isolating infected devices, blocking malicious traffic, and alerting security personnel.
6) *Collaboration:* IoT devices can facilitate collaboration between different security teams and stakeholders, such as law enforcement, industry groups, and academia, to share information and best practices in combating cybercrimes.

VII. CONCLUSION

In conclusion, since the amount of linked devices keeps increasing, there is an increasing concern about the role that IoT plays in cybercrimes. The imperfections in today's IoT systems make them easy targets for cybercriminals, leading to data breaches, identity theft, and other cyber-attacks. However, by prioritizing security by design, implementing best practices for securing IoT devices, developing standards and regulations, and collaborating across the industry, government, and consumers, we can overcome the challenges associated with IoT security and mitigate the risks of cyber-attacks. It is essential that all stakeholders involved in the development, deployment, and use of IoT systems take proactive measures to prioritize IoT security, ensuring that these systems can continue to deliver their benefits without exposing users to unnecessary risks.

REFERENCES

[1] Garuba, M., & Atayero, A. A. (2018). IoT security: review, blockchain solutions, and open challenges. Future Internet, 10(10), 88.
[2] Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. Computer Communications, 54, 1-31. https://daneshyari.com/article/preview/448154.pdf
[3] Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. Computer, 44(9), 51-58. https://www.nics.uma.es/pub/papers/1633.pdf
[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7123563
[5] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56, 684-700. https://www.sciencedirect.com/science/article/pii/S0167739X15003015

[6] Zhou, J., Cao, Z., Dong, X., Vasilakos, A. V.(2017). Security and privacy for cloud-based IoT: challenges. IEEE Communications Magazine, 55 (1), 26-33. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7823334

[7] 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.

[8] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173. https://doi.org/10.4236/jcc.2015.35021

[9] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[10] Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. In: Proc. 14th IEEE annual consumer communications & networking conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017. https://doi.org/10.1109/ccnc.2017.7983271.

[11] Yehia, L., Khedr, A. and Darwish, A. (2015) Hybrid Security Techniques for Internet of Things Healthcare Applications. Advances in Internet of Things, 5, 21-25. https://doi.org/10.4236/ait.2015.53004

[12] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. IEEE Communications Surveys & Tutorials, 16(1), 414-454.

[13] Arseni, S.C., Halunga, S., Fratu, O., Vulpe, A. and Suciu, G. (2015) Analysis of the Security Solutions Implemented in Current Internet of Things Platforms. IEEE Grid, Cloud & High Performance Computing in Science, Romania, 28-30 October 2015, 1-4. https://doi.org/10.1109/ROLCG.2015.7367416

[14] Wang, R., Wang, J. and Wang, N. (2015) Analysis of Key Technologies in the Internet of Things. 3rd International Conference on Material, Mechanical and Manufacturing Engineering, Guangzhou, 27-28 June 2015, 938-941. https://doi.org/10.2991/ic3me-15.2015.180

[15] Weber, R.H. (2010) Internet of Things—New Security and Privacy Challenges. Computer Law and Security Review, 26, 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

[16] Gendreau, Audrey A., and Michael Moorman. "Survey of intrusion detection systems towards an end to end secure internet of things." In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud), pp. 84--90. IEEE, 2016. https://ieeexplore.ieee.org/abstract/document/7575848

[17] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," 2017 2nd International Conference on Anti-Cybercrimes (ICACC), Abha, Saudi Arabia, 2017, pp. 93-97, doi: 10.1109/Anti-Cybercrime.2017.7905270. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7905270&isnumber=7905252

[18] Yang Lu and Li Da Xu, (2019) Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, IEEE Internet of Things Journal ,Volume: 6 , Issue: 2 , pp- 2103 – 2115 https://ieeexplore.ieee.org/document/8462745

[19] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia, 2017, pp. 93-97, doi: 10.1109/Anti-Cybercrime.2017.7905270. URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7905270&isnumber=7905252

[20] M. Schiefer, "Smart Home Definition and Security Threats," in 2015 Ninth International Conference on IT Security Incident Management & IT Forensics (IMF), Magdeburg, Germany, 2015 pp. 114-118. doi:10.1109/IMF.2015.17 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7195812

[21] Hilt, S.; Kropotov, V.; Merces, F.; Rosario, M. and Sancho, D. (2017) The Internet of Things in the Cybercrime underground, Trend Micro Research,pp-1-https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf

[22] L. D. Xu, W. He and S. Li, "Internet of Things in industries: A survey", *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233-2243, Nov. 2014 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6714496

[23] Yang Lu and Li Da Xu, (2019) Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, IEEE Internet of Things Journal ,Volume: 6 , Issue: 2 , pp- 2103 – 2115. https://ieeexplore.ieee.org/document/8462745 M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta, S. Singh, "A Review on Cyber Crimes on the Internet of Things"in arxiv.submitted on september 12 2020. 2009.05708.pdf (arxiv.org)

[24] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," in Computer, vol. 44, no. 9, pp. 51-58, Sept. 2011, doi: 0.1109/MC.2011.291.https://ieeexplore.ieee.org/document/6017172

[25] C. Lai, R. Lu, D. Zheng, H. Li and X. Shen, "Toward Secure Large-Scale Machine-to-Machine Communications in 3GPP Networks", *IEEE Comm. Magazine Supplement*, pp. 12,December 2015 . https://ieeexplore.ieee.org/document/7355579

[26] R. T. Tiburski, L. A. Amaral, E. de Matos and F. Hessel, "The Importance of a Standard Security Architecture for SOA - Based IoT Middleware", *IEEE Communications Magazine*, December 2015. https://ieeexplore.ieee.org/document/7355580

[27] M. Libicki, "The coming of cyber espionage norms," 2017 9th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2017, pp. 1-17, doi: 10.23919/CYCON.2017.8240325. https://ieeexplore.ieee.org/document/8240325

[28] W. T. Zhu, "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme," 2011 International Conference on Network Computing and Information Security, Guilin, China, 2011, pp. 156-160, doi: 10.1109/NCIS.2011.130.

[29] Q. Li, H. Li, Z. Wen and P. Yuan, "Research on the P2P Sybil attack and the detection mechanism," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2017, pp. 668-671, doi: 10.1109/ICSESS.2017.8343002.

[30] N. AlDossary, S. AlQahtani and H. AlUbaidan, "A Survey on Resource Management and Security Issues in IoT Operating Systems," 2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia, 2022, pp. 26-30, doi: 10.1109/WiDS-PSU54548.2022.00017.

[31] J. R. Wallrabenstein, "Practical and Secure IoT Device Authentication Using Physical Unclonable Functions," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 2016, pp. 99-106, doi: 10.1109/FiCloud.2016.22.

[32] H. Kim, A. Wasicek, B. Mehne and E. A. Lee, "A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 2016, pp. 114-122, doi: 10.1109/FiCloud.2016.24.

[33] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

[34] W. Lv, F. Meng, C. Zhang, Y. Lv, N. Cao and J. Jiang, "A General Architecture of IoT System," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2017, pp. 659-664, doi: 10.1109/CSE-EUC.2017.124.

[35] H. N. Saha, A. Mandal and A. Sinha, "Recent trends in the Internet of Things," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017, pp. 1-4, doi: 10.1109/CCWC.2017.7868439.

[36] C. Bahhar, C. Baccouche, S. Ben Othman and H. Sakli, "Real-time intelligent monitoring system based on IoT," 2021 18th International Multi-Conference on Systems, Signals & Devices (SSD), Monastir, Tunisia, 2021, pp. 93-96, doi: 10.1109/SSD52085.2021.9429358.

Dr.Sanyam Agarwal is a highly experienced professional with over 29 years of expertise in his area. He is currently working as a Professor and Director at ACE College of Engineering & Management in Agra, India. He has made significant contributions to his field through his extensive research and publications in national journals and conferences. Dr. Agarwal has completed his B.Tech, M.Tech, and Ph.D. degrees, and has also worked as a marketing executive and country head in MNCs for seven years after graduation. He is a member of many societies, including the World Semiconductor Forum, and serves as the editor of the journals JOTSSN & IJARSE. He has also been an editor for his book published by CRC Publisher and has written several textbooks on different topics. Dr. Agarwal's research area is in communication networks and the Internet of Things, and he has published one patent and worked as subject matter expert. He has been reviewer and guest speaker at many conferences. He has achieved numerous awards for his work in diverse fields. He has made significant contributions in the field of engineering and technology.

Mr. Veer Daksh Agarwal is a B.tech third-year computer science engineering student at the Thapar Institute of Patiala, India. He is trying to achieve top positions for society at his institution and has already achieved a number of milestones via competing in and winning the top 10 student Code for Good competition. He is a motivated individual who enjoys learning new things. Nothing is impossible, in his opinion. He is quite interested in machine learning, AI, and IOT**.**

Er. Vipin Mittal is a highly skilled professional with over 28 years of experience in his field, mostly in electronics and communication engineering. He is now employed as an assistant professor at IIMT University in Meerut. He holds an M.Tech. and a BE. Through his thorough study and publications in national magazines and conferences, he has significantly contributed to his area. He belongs to the International Association of Engineers. He has won numerous awards for his work in a variety of fields, including the Certificate of Appreciation from the IIMT University in Meerut in 2023, the IP Awareness/Training programme from the Government of India's NIPAM in 2023, the Faculty Development Programme from the School of Engineering & Technology in 2022, and the 30-day master class on electric vehicle design from Pantech e-Learning in Chennai in 2022. He has provided a variety of services to his field.

Mr. Ishaan Agarwal is a first-year B.Tech student at the SRM Institute of Science and Technology in Kattankulathur, Chennai. He is majoring in computer science engineering. He has a strong desire to learn and try new things. He is particularly interested in learning about the many branches of computer science and engineering. He has a strong sense of self-motivation and curiosity. He is engaged in cutting-edge work in the internet of things.