Secure Internet of Behavior (IOB): challenges and future Directions

SIDDHARTH SINGH KHATI[1],SUNIL K SINGH[2], AKASH SHARMA[3]

[1]UG Scholar, Chandigarh College of Engineering and Technology, Chandigarh
[2]Chandigarh College of Engineering and Technology, Chandigarh
[3]UG Scholar, Chandigarh College of Engineering and Technology, Chandigarh

ABSTRACT A wide discipline that may be used to study this development is required given the rapidly growing pervasiveness and integration of computers in human civilization. It is essential to maintain security throughout the process since the design and use of technology requires the development and application of models of humans and machines in all their features, including cognitive and memory models as well as social impact and (fake) emotions. Internet of Behaviours (IoB) seeks to explain how data are more efficiently analyzed and deployed to build and promote new goods from the standpoint of human psychology. Organizations can use the IoB in a variety of ways, whether they are public or private, which can be exploited if security frameworks when the communication are not maintained. The Internet of Behaviour, also known as IoB, is a concept that combines technology, human psychology, and the best aspects of data analysis, behavioral analysis, and technology. The IoB platform gives businesses the tools they need to create the thorough understanding of their clientele. Connecting gadgets to the Internet of things produces a lot of new data points (IoT). The objective of the IoB is to observe, analyses, understand, and react to all types of human behaviors in a way that enables people to be monitored and understood utilizing evolving technology and improvements in algorithms.

KEYWORDS Internet of Behaviours (IoB); IoT

I. INTRODUCTION

IoB is an IoT use case that concentrates on encouraging customers to enhance specific outcomes. IoB can be seen as the meeting point of three pillars [1]:

(a) Internet of Things: Provides client information such as location, daily schedule, health status, etc.
(b) Consumer psychology: Investigates the driving forces behind people's behaviors [2].
(c) Data analytics: To identify patterns of behavior and offer suggestions, algorithms can mix IoT data with psychological studies.

Based on the aforementioned points, use these three factors to achieve long-term client satisfaction and higher earnings. IoT is regarded as one of the most critical security flaws that affects almost everyone, including businesses, governments, and consumers. The risks associated with IoTsystems are unmatched despite all the benefits and value they provide. IoT security is crucialbecause connected devices give hackers a broad and easy-to-access attack surface. For thesevulnerable devices, IoT security and embedded architecture in IoT offers the essential protection required [3] [4], [28]. The functionality of the devices is the primary concern for IoT system developers, not security. Itis now even more crucial to deploy security measures, and users and IT teams should be in charge of doing so.

Industrial control system is a phrase related to OT (ICS). Robots, wind turbines, and cargo ships can all be operated effectively with the help of industrial control systems, which also incorporate devices and networking capabilities even through mobiles [5], [29]. If an IoT device is used to control a physical system, such as a device on the factory floor or a part of the power grid, it is referred to as an OT device.

Cybercriminals frequently use IoT and OT devices, which is a problem. perhaps even more than we do. The fundamental issue with IoT and ICS devices is that they make it possible for people or organizations to conduct cutting-edge cyberattacks. Hackers will employ any and all tactics necessary to attack a company, a neighborhood, or even a whole country [6] [7], [30].

Cybersecurity experts frequently make this claim, claiming that IoT expands the attack surface available to criminals. Security experts handle the resulting security threats since they are aware of this. [8], [31] Security evaluations that assess the complexity of parallelization and the possibility for enhanced parallelism to improve performance. [9], [32]

II. LITERATURE REVIEW

Having a secure network is essential for every IoT system. In recent years, there have been numerous cyber security threats Security of IoT networks has become even more crucial with the incorporation of SD Networking, big data [10], [33], soft computing and parallelization [11]. The security

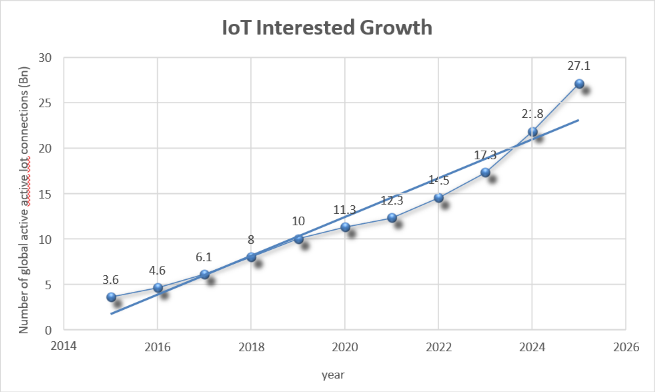

FIGURE 1: projected growth of global active IoT user from 2014 to 2026 (in Billions)

of IoT devices and edge layers has been extensively studied. There has been extensive research done on the protocols needed for machine-to-machine communication, CNN based approach and its security and privacy problems [12], [34]. There could still be harmful data on a trustworthy device, though. Machine learningmodels are useful in these situations because they treat each file as a separate sample point. In-depth analyses of the function of machine learning tools in IoT networks have been conductedin a number of models and studies. Author in [13], [35] suggested an IoT security approach based on parallelization and RFID tags.The author suggested for a strategy to safeguard IoT devices [14]. In a different publication, author [15] also recommended an IoT wireless protection strategy. The author made a suggestion for Behavior aware Privacy for IoT in. originator of the IoT-based federated learning strategy in [16].

III. THE KEY CHALLENGES OF INTERNET OF BEHAVIORS

IoT devices were not created with security in mind. As a result, there are numerous IoT security issues that can have severe consequences [17], [36]. IoT security is governed by a relatively small number of standards and laws compared to other technology solutions. The majority of people are also ignorant of the risks associated with IoT systems. Additionally, they are unaware of the magnitude of IoT security concerns. Some of the numerous IoT security concerns are Lack of visibility, Limited security integration, Open-source vulnerabilities. It is necessary to develop and manage IoT security in an integrated manner in order to effectively address IoT security challenges. It must take into account a range of strategies and instrumentsas well as neighboring systems, such as networks [18], [37].

The following are the key challenges of the IoB:

a. Manipulation for Profit: Let's go back to the person who wishes to stick to their diet as an example. if this person has a completely healthy body but is persuaded to starta diet by a healthcare professional. For instance, it would be possible to persuade people to spend more on healthcare if they have excessive health concerns.

b. Manipulation for control: Political parties or governments can use IoB to influence the populace.

c. Privacy concerns: It might be challenging to maximize profits because big data analysis and storage include a lot of sensitive personal data which requires high performance. Despite the increased regulation ofthe use of private data, there are technologies that enable data processing without disclosing private information [19], [38].

d. Laws and regulations: Regulations have not kept up with the development of technology. Legal problems still need to be overcome. Data security practises, for example, are not frequently standardized.

e. Threat from cyberattacks: As our reliance on digital technologies increases in our daily lives, so does our vulnerability to them. Despite the growth of cybersecurity tools and even insurances, people still need to consider these risks.

f. Persuading people to share their data: Some people might not wish to reveal their private information. Let's examine the situation of auto insurance. 47% of drivers don't want their driving information to be shared, according to Deloitte. Driving data includes details like average speed, amount of full brakes used per kilometer, driving routes, etc [20], [39].

IV. FUTURE OF INTERNET OF BEHAVIOR

By 2025, according to Gartner, more than half of all humans will interface with IoB systems operated by governments or private businesses. Smartphones can be purchased with IoB health apps like SoberTool, Noom, SmokeFree, and Health2Sync, the latter of which aids in the management of diabetes through blood glucose and activity tracking. IoB systems and apps of this nature will spread despite worries about data privacy [21], [40].

The popularity of e-commerce, digital assistants, social media platforms, and other technologies that demand personal information demonstrates that the majority of users will feel at ease supplying behavioral data as well. This opens the door for IoB to reinvent how businesses and organizations use technology to engage with and influence people [22], [41].

There are other technology and people options available. Here are a few techniques IT professionals may use to strengthen their IoT device security posture.

(a) Improve device monitoring: Information sharing and the usage of intrusion detection systems (IDS) and security information and event management (SIEM) systems can both be helpful. It is possible to profile attackers and more intelligently place security controls for IoT and ICS devices by using cybersecurity threat intelligence (CTI).

(b) Increase security features: Including features like capability that encrypts all transferred and stored data can be beneficial. Additionally, improved authentication protocols can support connection management. Employees can segregate themselves as well, which will help them react to security breaches more skillfully [23], [42].

(c) Observe IoT and ICS guidelines: The National Institute of Standards and Technology (NIST) has released numerous cybersecurity.

V. SECURING THE INTERNET OF THINGS ECOSYSTEM

Securing IoT devices is a challenging issue in and of itself for a number of reasons. Security usually receives a lower priority than time-to-market considerations since manufacturers and inventors are under pressure to produce new products. Many businesses are also unaware of the dangers that come with IoT and are typically more focused on the savings, convenience and automations that it offers [24], [43].

IoT will likely be employed in more than 25% of enterprise attacks by 2020, according to Gartner. In particular, industrial Internet of Things (IoT) systems face significant stakes. The operational risks in anything from national power generation and distribution infrastructures to international industrial operations may be significantly increased by connected IoT sensors and devices. Safeguarding the devices themselves is one option. For instance, some pieces of equipment may operate continuously without being watched, yet they still need to be secured. These devices can be made more resistant by adding tamper-evident and tamper-proof measures, which will stop potential attackers from taking over or accessing important information especially in the application of IoT in automated transportation [25], [44].

Enterprises must make sure that their IoT networks are secure in addition to protecting specific IoT devices. Strong user authentication and access control measures can be employed to assist make sure that only authorized users have access to the IoT framework.

VI. BEHAVIORAL INTERNET AND CYBERSECURITY

However, there is a dark side to IoT, according to experts, and the integration of behavior data might provide attackers access to private information that discloses consumer behavior patterns. Hacker-obtained delivery routes, bank access codes, and property access codes can all be collected and sold to other thieves; the possibilities are limitless. The other possibility isthat they will be able to better impersonate people for fraudulent or other bad intentions, raisingthe bar for "Phishing." [26]

New cybersecurity protocols are being developed as a result of the fast-growing network of IoT devices, and enterprises must be ever more proactive and attentive. According to researcher and technology author Chrissy Kidd's post on the BMC blog, "Many people prefer having their gadgets synced and derive benefits and ease from this setup. The Internet of Things is not inherently hazardous. The issue is rather how we obtain, organize, and make use of the data, especially at scale. And we're beginning to comprehend this issue. She goes on to say that the IoB method, which links our data with our legal and cultural norms must change in order for our decision-making to be effective.

"Your interactions with a particular business are just one source of data collection for the IoT. An auto insurance provider, for instance, would review a summary of your driving record. We've concluded that this is fair as a society. However, the insurers might also examine your social media connections and profiles to "predict" if you're a safe driver—a dubious and illegal practices. Companies can easily connect your smart phone to your laptop, home voice assistant, home or car cameras, and possibly your cell phone records (texts and phone calls) [27]. Additionally, it goes beyond the actual equipment. Many businesses secretly share(sell) data with other divisions or across corporate borders. Continued software acquisitions byGoogle, Facebook, and Amazon, usually without our consent, have the potential to integrate users of a single app into their whole online ecosystem. Kidd claims that these worries are not adequately protected by the law. As a result, there are major security and legal dangers.

VII. CONCLUSION

The Internet of Behaviors offers Innovative strategies for marketing products and services and influencing customer and staff behavior that are available to the organizations. By relying on the data that has been acquired, organizations can use this technology to significantly improve their customer interactions. IoB has evolved into a worldwide setting that categorizes human behavior. IoB analyses behavioral data before determining its potential. In order to develop methods for producing and selling things to consumers, businesses have examined, tested, and used a variety of methodologies. A safe network for people, software/hardware, processes, and things is what the Internet of Things (IoT) is guaranteed to be thanks to cybersecurity. If that's the case, IoT will provide a higher degree of interoperability, confidentiality, scalability, availability, and integrity. IoT will also be primarily focused on addressing cybersecurity challenges in the next years.

REFERENCES

[1] Buente, W., & Robbin, A. (2008). Trends in Internet information behavior, 2000–2004. Journal of the American Society for Information Science and Technology, 59(11), 1743-1760.

[2] Javaid, M., Haleem, A., Singh, R. P., Rab, S., & Suman, R. (2021). Internet of Behaviours (IoB) and its role in customer services. Sensors International, 2, 100122.

[3] Sunil Kr Singh, R. K. Singh and M. Bhatia, "Design flow of reconfigurable embedded system architecture using LUTs/PLAs," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, pp. 385-390, DOI: https://doi.org/10.1109/PDGC.2012.644985.

[4] Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.

[5] Peñalvo, F. J., Sharma, A., Chhabra, A., Singh, S. K., Kumar, S., Arya, V., & Gaurav, A. (2022). Mobile Cloud Computing and Sustainable Development: Opportunities, Challenges, and Future Directions. International Journal of Cloud Applications and Computing (IJCAC), 12(1), 1-20. http://doi.org/10.4018/IJCAC.312583

[6] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80, 1-50.

[7] Sunil Kr. Sharma, Sunil Kr. Singh, and Subhash Panja, "Human Factors of Vehicle Automation", in Autonomous Driving and Advanced Driver-Assistance Systems (ADAS): Applications, Development, Legal Issues, and Testing (1st ed.). CRC Press, Chapter15, pp335- 358, 2021. https://doi.org/10.1201/9781003048381

[8] Gupta S. et. al. (2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: Present and future challenges. International Journal of Cloud Applications and Computing, 7(3), 1–43.

[9] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

[10] Chahid, Y., Benabdellah, M., & Azizi, A. (2017, April). Internet of things security. In 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS) (pp. 1-6). IEEE.

[11] Kumar, S., Singh, S. K., Aggarwal, N., & Aggarwal, K. (2021). Evaluation of automatic parallelization algorithms to minimize speculative parallelism overheads: An experiment. Journal of Discrete Mathematical Sciences and Cryptography, 24(5), 1517–1528. https://doi.org/10.1080/09720529.2021.1951435

[12] Sudhakar Kumar, Inderpreet Singh, Sunil Kr. Singh, Kriti Aggarwal (2021), "Dropout- VGG based Convolutional Neural Network for Traffic Sign Categorization", in the proc. of 2nd Congress on Intelligent Systems (CIS 2021), Lecture Notes on Data Engineering and Communication Technologies. Springer, Berlin, Heidelberg.

[13] Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things.Computer, 44(9), 51-58.

[14] Kumar, S., Singh, S. K., Aggarwal, N., Gupta, B. B., Alhalabi, W., & Band, S. S. (2022). An efficient hardware supported and parallelization architecture for intelligent systems to overcome speculative overheads. International Journal of Intelligent Systems.

[15] C. L. Stergiou and et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," in Handbook of computer networks and cyber security. Springer, 2020, pp. 525–554.

[16] Z. Lv, "Security of internet of things edge devices," Software: Practice and Experience, vol. 51, no. 12, pp. 2446–2456, 2021.

[17] J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," Computer Communications, vol. 97, pp. 1–14, 2017.

[18] V. Gazis, "A survey of standards for machine-to-machine and the internet of things," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 482–511, 2016.

[19] Singh, S. K., Kaur, K., Aggarwal, A., & Verma, D. (2015). Achieving High Performance Distributed System: Using Grid Cluster and Cloud Computing. Int. Journal of Engineering Research and Applications, 5(2), 59-67.

[20] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, and M. Stanley, "A brief survey of machine learning methods and their sensor and iot applications," in 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA). IEEE, 2017, pp. 1– 8.

[21] K. Singamaneni, G. Dhiman, S. Juneja, G. Muhammad, S. AlQahtani, and J. Zaki, "A novel qkd approach to enhance iot privacy and computational knacks," Sensors, vol. 22, no. 18, 2022.

[22] M. Chehab and A. Mourad, "Lp-sba-xacml: Lightweight semantics based scheme enabling intelligent behavior-aware privacy for iot," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 161–175, 2022. [Online].

[23] S. Abdulrahman, H. Tout, A. Mourad, and C. Talhi, "Fedmccs: Multicriteria client selection model for optimal iot federated learning," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4723–4735, 2021. [Online].

[24] B. B. Gupta and M. Quamara, "Decentralised control-based interaction framework for secure data transmission in internet of automated vehicles," International Journal of Embedded Systems, vol. 12, no. 4, pp. 414–423, 2020.

[25] Gupta, A., Singh, S. K., & Gupta, A. (2021, December). A novel Smart Transportation based framework interlinking the advancements in Technology and System Engineering. In International Conference on Smart Systems and Advanced Computing (Syscom-2021).

[26] F. Mirsadeghi and et al., "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," Peer-to-Peer Networking and Applications, vol. 14, no. 4, pp. 2537–2553, 2021.

[27] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," IEEE Transactions on Intelligent Transportation Systems, 2021.

[28] Chui, K. T., et al. (2022). An MRI scans-based Alzheimer's disease detection via convolutional neural network and transfer learning. Diagnostics, 12(7), 1531.

[29] Mishra, A., et al. (2021, January). Classification based machine learning for detection of ddos attack in cloud computing. In 2021 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-4). IEEE.

[30] Tewari, A., et al. (2018, January). A mutual authentication protocol for IoT devices using elliptic curve cryptography. In 2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence) (pp. 716-720). IEEE.

[31] Gupta, B. B., et al. (2018). Assessment of honeypots: Issues, challenges and future directions. International Journal of Cloud Applications and Computing (IJCAC), 8(1), 21-54.

[32] Tewari, A., et al. (2020). An analysis of provable security frameworks for RFID security. In Handbook of computer networks and cyber security (pp. 635-651). Springer, Cham.

[33] Dahiya, A., et al. (2021). How IoT is Making DDoS Attacks More Dangerous.

[34] Chui, K. T., et al. (2021). Extended-range prediction model using NSGA-III optimized RNN-GRU-LSTM for driver stress and drowsiness. Sensors, 21(19), 6412.

[35] Agrawal, D. P., et al. (2018). Recent advances in mobile cloud computing. Wireless Communications and Mobile Computing, 2018.

[36] Gupta, B. B., et al. (2022). Novel Graph-Based Machine Learning Technique to Secure Smart Vehicles in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems.

[37] Gupta, S., et al. (2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. International Journal of Cloud Applications and Computing (IJCAC), 7(3), 1-43.

[38] Alsmirat, M. A., et al. (2017). Accelerating compute intensive medical imaging segmentation algorithms using hybrid CPU-GPU implementations. Multimedia Tools and Applications, 76(3), 3537-3555.

[39] Gupta, B. B., et al. (2015). Cross-site scripting (XSS) abuse and defense: exploitation on several testing bed environments and its defense. Journal of Information Privacy and Security, 11(2), 118-136.

[40] Gupta, S., et al. (2015, May). PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications. In Proceedings of the 12th ACM international conference on computing frontiers (pp. 1-8).

[41] Mishra, A., et al. (2011, September). A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques. In 2011 European Intelligence and Security Informatics Conference (pp. 286-289). IEEE.

[42] Jain, A. K., et al. (2018). PHISH-SAFE: URL features-based phishing detection system using machine learning. In Cyber Security (pp. 467-474). Springer, Singapore.

[43] Tewari, A., et al.. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. International Journal of Advanced Intelligence Paradigms, 9(2-3), 111-121.

[44] Kaur, M., et al. (2021). Secure and energy efficient-based E-health care framework for green internet of things. IEEE Transactions on Green Communications and Networking, 5(3), 1223-1231.