Actor-Network Theory Applied to Internet of Things (IoT) Devices: A Possible Data Privacy and Security Threat

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Aryan Sawhney

Fall 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

The transformative impact of the Internet of Things (IoT) is undeniable, enhancing areas from remote patient monitoring in healthcare to energy optimization in smart homes. In the research paper, *All Things Considered: An Analysis of IoT Devices on Home Networks*, the authors provide an analysis of IoT devices in real-world homes by leveraging data collected from user-initiated network scans of 83M devices in 16M households (Kumar et al., 2019). They determined that IoT adoption is widespread: to the point that on several continents, there are more than half of the households already have at least one IoT device. Yet, this rapid technological advancement comes with complex privacy and security implications. Many IoT devices collect enormous amounts of data from healthcare, manufacturing, industrial IoT, smart homes, smart cities, and so on (Khare & Totaro, 2019). These IoT devices are often shipped with easily guessable default passwords, rendering them vulnerable to unauthorized access (Aziz Al Kabir et al., 2023). These two issues create a perilous situation in which sensitive data is highly susceptible to unauthorized access. When multiple devices collect various data points, the aggregation of this information can reveal sensitive and private aspects of a user's life, such as sexual orientation, political beliefs, and even the use of addictive substances (Choi et al., 2019).

The repercussions are significant and multifaceted. For individuals, the risk of identity theft has been on the rise. According to a study on identity theft conducted in 2005, 8.3 million people faced some form of identity theft (Anderson et al., 2008). Beyond financial risks, there are broader societal concerns, including the potential for stalking or unauthorized surveillance. Businesses also face severe consequences; not only do they risk legal repercussions but they also face the deprecation of consumer trust, which could potentially stifle future innovations. Additionally, Cybercriminals frequently focus on IoT devices because they serve as entry points

to other interconnected systems and can be exploited to establish botnets (a network of computers that have been linked together by malware (Merriam-Websetrs)) or conduct man-in-the-middle attacks (An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them (Franklin et al. 2020)). Therefore, the lack of security in IoT devices raises a multitude of issues regarding privacy and safety.

This paper, argues that measures must be taken to successfully navigate the ever-changing IoT environment to maintain user safety and privacy while still retaining an influential role in daily life. This paper analyzes IoT devices through the lens of Actor-Network Theory to understand the vulnerabilities and effects of IoT devices.

The Prevalence of Internet of Things Devices and Their Risks

To understand the actors involved in IoT devices, this paper reviews sources that evaluate the presence of IoT devices, their security features, and the potential risks they harbor. The Internet of Things has rapidly integrated into various facets of human life, marking a transformative shift in how we interact with technology. The adoption of IoT devices is now a global phenomenon, affecting millions of households and multiple sectors. Recent studies indicate that more than half of households across several continents have already incorporated at least one IoT device, whether it be a smart thermostat, wearable fitness tracker, or a more complex system like home security (Kumar et al., 2019). This surge in adoption is not just confined to consumer applications; industries such as healthcare, manufacturing, and energy are also deploying IoT technologies for everything from remote patient monitoring to supply chain management.

What makes IoT devices especially interesting is their versatility and the range of functionalities they offer. In the healthcare sector, for instance, “The Internet of Things is an emerging technology that provides enhancement and better solutions in the medical field, such as proper medical record-keeping, sampling, integration of devices, and causes of diseases.” (Javaid & Khan, 2021) These advancements could be seen during the COVID-19 pandemic, where they played a crucial role in enabling us to combat and contain the virus. Similarly, smart homes equipped with IoT devices offer unprecedented levels of convenience and efficiency. This is further shown when the FTC states, “Internet of Things (IoT) companies design, manufacture, market, or support these connected devices – everything from light bulbs to smart TVs to wearable fitness trackers,” (Ritchie & Jayanti, 2021). In the industrial sector, IoT devices monitor machinery, predict maintenance needs, and manage resources, demonstrating the wide array of applications that these devices have in modern life (Xu et al., 2018).

However, the accelerated growth of IoT adoption also means that more aspects of daily life are becoming dependent on these connected systems. While this creates avenues for increased efficiency and improved quality of life, it also poses challenges, especially concerning security and privacy. As these devices become increasingly ever-present, understanding the scale and depth of their implementation into daily routines is crucial for addressing the potential risks they bring. The wide adoption of IoT devices not only showcases human ingenuity but also underscores the imperative for responsible innovation that considers the long-term implications on user data and safety.

The rapid rise in the adoption of IoT devices has been accompanied by an equally concerning trend, lax security measures. Aziz specifically references the consequences of these inadequate security measures when talking about IOT devices, “Typically more vulnerable to a

range of security threats such as using default passwords that can be easily compromised by attackers – which in turn will then allow them to use the compromised device to launch attacks on other connected devices or networks, being stuck with outdated firmware that may be susceptible to known vulnerabilities, lacking secure boot mechanisms – which would allow attackers to modify the device's firmware and gain persistent access, and lacking encryption." (Aziz Al Kabir et al., 2023) We can further see the prevalence of threats in Figure 1, which illustrates the wide variety of security threats that have been used on IoT devices. Whether it's a home security camera, a smart thermostat, or an industrial control system, these weak security settings create open doors for cybercriminals.

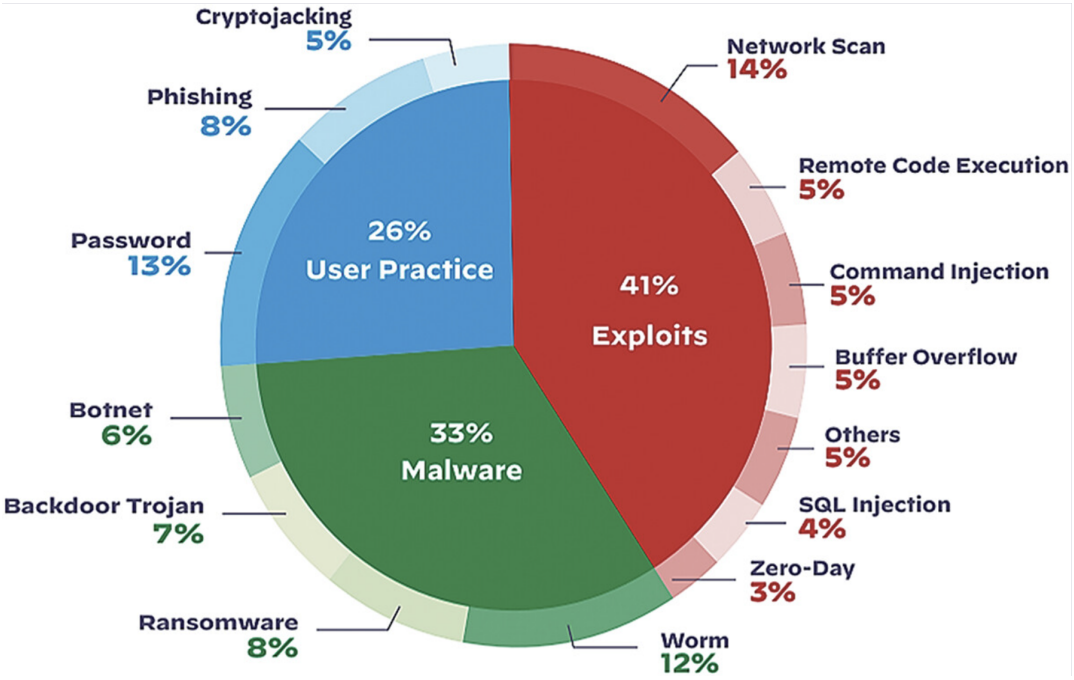

Figure 1–A pie-chart of the most common threats and attacks on IoT devices. (Aziz Al Kabir et al., 2023)

The consequences of these inadequate security features can be far-reaching and multi-layered. On an individual level, the risk is not merely the unauthorized control of a device but also the potential exposure of sensitive data. Given that many IoT devices collect an array of

information, from our daily routines to health metrics, the aggregation of such data can reveal intimate aspects of a person's life. In the hands of cybercriminals, such aggregated information can not only compromise a person's privacy but can also be weaponized in various ways, such as identity theft, financial fraud, or even for blackmail purposes. For instance, the data from a smart home system can provide a detailed account of an individual's daily routine, thereby making it easier for criminals to plan burglaries or other targeted attacks. The increase in ease for these criminals has also caused the "Average cyber insurance claim to rise from USD 145,000 in 2019 to USD 359,000 in 2020." (Cremer et al., 2022)

Beyond the individual, the poor security measures in IoT devices have repercussions that ripple through society and industry. One prominent concern is the loss of consumer trust. When a device is easily compromised, it erodes faith not only in the particular brand but in the technology as a whole, which can hamper innovation and market growth. Furthermore, businesses can face significant legal consequences for failing to secure user data adequately, as data breaches may violate various privacy laws and regulations. This adds a layer of financial risk, as businesses could find themselves facing hefty fines and costly litigation. An example of this was in November of 2018, when Marriott International Inc which was when, "A multinational hotel corporation, notified customers of a data breach resulting in the possible disclosure of credit cards, passport numbers, and other personally identifying info belonging to 300 million customers." (Biberstein & Rajesh, n.d.) Information breaches such as this can cause irreparable harm not only to the individuals affected but also to the company. The societal impact extends to critical infrastructure too; a compromised IoT device in a power grid or a water treatment facility can pose severe public safety risks. Aziz further emphasizes this when he states, "An overwhelmingly large number like this certainly adds a great deal of credibility to

their sheer pervasiveness, and it is safe to assume that the number of IoT devices will only continue to grow every year as we continue to find more practical applications for their use in numerous different fields such as, but certainly not limited to, healthcare, wearables, home entertainment, security (ironically), agriculture, shipping and tracking, transportation, city infrastructures, power generation, and retail as well as manufacturing industries." (Aziz Al Kabir et al., 2023)

Finally, the poor security measures of individual IoT devices can lead to broader cybersecurity threats. These devices often become part of large-scale Distributed Denial of Service (DDoS) attacks or serve as entry points for infiltrating secure networks. Since IoT devices are increasingly interconnected, a vulnerability in one can often be exploited to compromise others, leading to a chain reaction of security breaches. This interconnectedness also makes it possible for attackers to launch more sophisticated attacks such as man-in-the-middle attacks or to establish botnets, leveraging the compromised devices to carry out further cybercrimes (Aziz Al Kabir et al., 2023). The 2016 Mirai botnet attack exemplifies this, as it harnessed insecure IoT devices like security cameras and routers to launch a massive DDoS attack against major websites ("Individual Pleads Guilty," 2020).

It's also worth noting that the poor security landscape of IoT devices is not just a product of negligent design; it's partly a consequence of the rapid pace at which these devices are brought to market. Many manufacturers, in a rush to be first, may sideline security considerations, viewing them as secondary to functionality and user experience. Aziz proves this when he states, "As there are billions of IoT devices in use today, the sheer number of such devices pose a great security challenge as they are often constrained by several hardware and software limitations in addition to being designed with a focus on convenience, ease of use, mass production, and low

cost, rather than security."(Aziz Al Kabir et al., 2023) This approach, while potentially profitable in the short term, poses substantial risks to consumers and can ultimately act as a roadblock to the long-term success and evolution of IoT technologies. Thus, as we integrate more smart devices into our lives, the urgency for robust security measures cannot be overstated.

Despite the promise and prevalence of IoT technologies, we are still in a nascent stage of understanding effective mitigation strategies. Critical questions remain unanswered. What are the best practices for enhancing security measures in these devices? How can we educate consumers about the inherent risks tied to the use of unsecured IoT gadgets? Can industry standards or government regulations impose a minimum level of security features effectively? What role do manufacturers and software developers play in making sure these devices are not just smart but also safe? Addressing these questions is not just a technical necessity but an ethical imperative. The remainder of this paper will explore IoT devices using Active Network Theory as a framework, aiming to comprehensively understand their security vulnerabilities and their implications.

Method for Analyzing the Internet of Things: Actor-Network Theory

Understanding the intricate mechanisms and relationships within IoT is no trivial matter. Traditional models of analysis often fall short of capturing the dynamic interplay between human and non-human actors in this rapidly evolving field. It is in this context that Actor-Network Theory (ANT), a socio-technical framework that emerged from the field of Science and Technology Studies, offers an unprecedented depth of insight. This essay aims to examine the intricacies of IoT through the lens of ANT, providing a thorough understanding of how various elements interact within this complex system.

Actor-Network Theory

Actor-network theory (ANT) is a theoretical and methodological approach primarily developed in the field of science and technology studies by scholars like Bruno Latour, Michel Callon, and John Law (Tatnall, 2019). ANT posits that both human and non-human entities, referred to as "actors," participate in networks to bring about certain phenomena. Rather than considering technology or society as separate, fixed entities, ANT looks at how they are mutually constituted. It suggests that no actor operates in isolation, but is always part of a network that includes other human actors as well as objects like computers, documents, or even geographical spaces (Tatnall, 2019). In these networks, each actor contributes to shaping the outcome and no single actor has complete control over what happens. Figure 2 visually represents the Actor-Network Theory of Graphical User Interfaces, highlighting the interconnections between users and designers with various elements such as icons, applications, user input, and technical constraints, among others. In essence, ANT is a tool for analyzing the relationships and power dynamics within complex systems. It helps us understand how things come into being and how they are maintained through the interactions among various actors. By viewing all elements in a network as actors that both shape and are shaped by the network, ANT allows for a more nuanced understanding of complex social, technical, and natural phenomena (Arif et al., 2017).

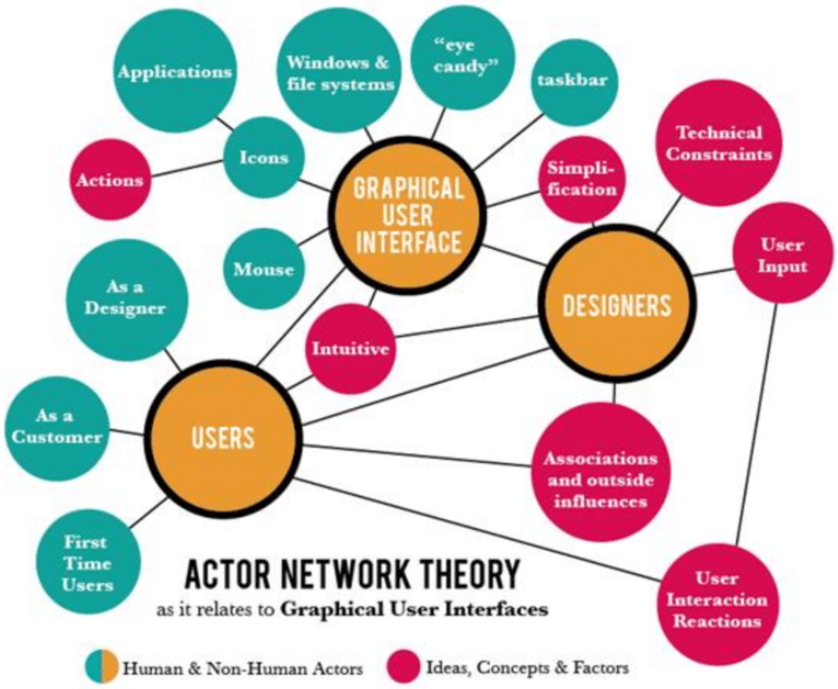

Figure 2–Actor-Network Theory illustrating the intricate relationships between various components of Graphical User Interfaces. (ResearchGate, n.d.)

The first step in this analytical journey involved identifying all the actors implicated in these IoT ecosystems. The term "actor" here is not confined to human entities but also includes non-human components like sensors, databases, and networking hardware. Next, the initial alliances or partnerships between these actors were mapped out to understand the preliminary framework of these networks. For example, user-friendly interfaces often align with the goals of end-users, while robust and flexible programming languages may be preferred by developers.

The stabilization of these networks was then observed, which involved scrutinizing how the alliances among various actors contributed to the stability or volatility of the network. For instance, an easy-to-use interface may garner more users, thereby stabilizing its position in the network. Finally, the network's growth trajectory was analyzed by observing the inclusion of new

actors, such as additional sensors or software updates, and how these new inclusions affected the overall stability and functionality of the network.

Actor-Network Theory for the Internet of Things

To comprehend why Actor-Network Theory is an effective framework for analyzing Internet of Things (IoT) devices, we will examine insights from our previous research on autonomous vehicles as a case study (Seuwou et al., 2016). This research aims to explore the complex factors that influence individual acceptance or rejection of autonomous vehicles as a disruptive technology. Leveraging a multi-disciplinary approach, the study employs Actor-Network Theory (ANT) as its foundational framework, augmented by interviews with experts across various fields and user surveys. By integrating ANT with existing models like the Technology Acceptance Model (TAM) (seen in Figure 3) and the Unified Theory of Acceptance and Use of Technology (UTAUT2), it aims to provide a comprehensive understanding that goes beyond mere technological features to include socio-economic, psychological, and cultural dimensions. Its approach culminates in a set of testable hypotheses that set the stage for future empirical research, seeking to address current gaps in the literature and offer a holistic view of technology adoption and usage (Seuwou et al., 2016).

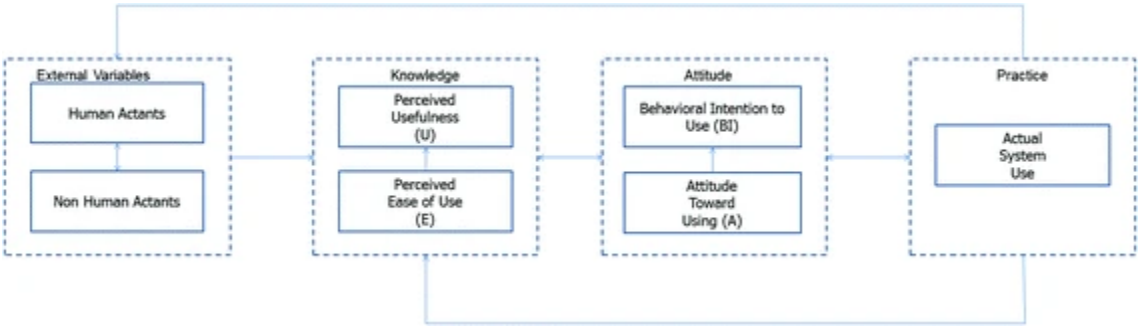

Figure 3–Combined TAM – ANT model. (Seuwou et al., 2016)

Actor-network theory (ANT) can be an equally potent analytical framework for examining the Internet of Things (IoT) as it has been for autonomous vehicles in the current research. Both contexts involve a complex interplay of human and non-human actants—ranging from individuals and organizations to sensors, software, and network protocols. Similar to autonomous vehicles, IoT devices also represent a disruptive technology that integrates into various aspects of human life and society. ANT allows for the scrutiny of these relationships in a nuanced way, taking into account not just the technological factors but also the social, economic, and psychological aspects that affect adoption and usage. Moreover, the capacity of ANT to ascribe agency to non-human actors is particularly relevant in the IoT context, where non-human elements like sensors and algorithms play a critical role. Thus, ANT provides a comprehensive and adaptable framework well-suited to the multifaceted challenges posed by IoT technologies.

Actor-network theory (ANT) is a particularly apt framework for analyzing Internet of Things (IoT) systems because it recognizes the complexity and dynamism inherent in these networks. IoT environments consist of multiple interacting elements—sensors, devices, platforms, and human users—that collectively contribute to the system's functionality. Traditional models that focus solely on human actors or technological components are often inadequate for capturing the full scope of relationships and influences at play. ANT offers a more holistic view by treating all elements, whether human or non-human, as actors within a network that both influence and are influenced by each other. This allows for a nuanced understanding of how different components interact, what roles they play, and how power dynamics shift within the network, ultimately providing valuable insights for improving system performance, security, and user experience.

Both the Actor-Network Theory framework and the multifaceted evidence considered are extremely relevant for this analysis. ANT enables a nuanced examination of both human and non-human actors on an equal footing, while the evidence offers concrete data to inform this analytical process. The combination of this framework and evidence yields valuable insights into the complexities of IoT networks. These insights can potentially guide better design and implementation practices, thereby contributing to more reliable and efficient IoT systems in the future.

Results: Analyzing the Internet of Things (IoT) Through the Lens of Actor-Network Theory

ANT posits that actors participate in the creation and maintenance of social networks. These actors, through their interactions and relationships, shape the trajectory and impact of technological innovations. This perspective is particularly relevant for understanding the Internet of Things (IoT), an ever-expanding ecosystem where physical devices—ranging from household appliances to industrial sensors—are interconnected and capable of sharing data. By employing ANT, this paper aims to unravel the intricate web of actors and alliances that constitute the IoT landscape, thereby providing nuanced insights into its development, challenges, and societal implications.

Human Actors

In the intricate web of the Internet of Things (IoT), human actors play diverse and critical roles. These range from engineers and developers who design and code IoT devices to consumers who use smart devices in their daily lives, and policymakers who create regulations

governing data and security. Each group of human actors has its own set of interests, goals, and expectations, which they bring into the actor network. For example, engineers may focus on innovation and efficiency, consumers on ease of use and utility, and policymakers on ethical and legal implications. Importantly, the choices and actions of these human actors have a profound impact on the formation and stabilization of the network. Through Actor-Network Theory, we see that these human actors are not passive recipients but active participants, continually shaping and reshaping the network's architecture, functionality, and impact on society.

Non-Human Actors

Additionally, non-human actors in the Internet of Things are not merely passive components but active agents that influence the dynamics of the network. These include the physical IoT devices themselves, such as smart thermostats, wearables, and connected vehicles, as well as the software algorithms and data repositories that enable them. For instance, a smart thermostat learns from user behavior to adjust room temperatures automatically, impacting energy consumption and user comfort. Software algorithms sift through immense data streams to flag irregularities, thereby enhancing security. These non-human actors have "agency" in that they make decisions, often autonomously, that affect the entire network's performance and stability. Their complex interactions with human actors and each other create a multi-layered, interconnected ecosystem, full of both possibilities and vulnerabilities.

Initial Alliances

As IoT devices multiply, initial alliances that shape their development and deployment come into focus. Manufacturers often form partnerships with software developers to ensure that their hardware is optimized for specific applications and functionalities. These alliances are crucial for creating IoT devices that are not only robust but also user-friendly. On another front,

policymakers may align with consumer protection agencies to establish regulatory guidelines that aim to secure data and uphold user privacy. This often comes in response to alliances among privacy advocacy groups and concerned users, who press for stringent regulations. Meanwhile, networking companies providing the backbone infrastructure may create alliances with cloud service providers, optimizing the efficiency and scalability of data storage and management. Within the IoT ecosystem, the devices themselves often form alliances in a sense; for example, smart home devices from the same manufacturer or compatible third-party brands are designed to work in harmony. These relations can be further observed in Figure 4. This synergy allows for a more integrated and automated user experience. It is through these alliances, both explicit and implicit, that the stage is set for the IoT's technological trajectory, defining how it interacts with society and vice versa.

Figure 4–Alliances between different actors related to IoT devices. (created by author)

Stabilization

As IoT technologies mature, a phase of stabilization emerges where certain norms, protocols, and standards gain widespread acceptance, facilitating more robust and seamless interactions among actors. Within this stabilized network, prominent actors—such as leading technology firms, regulatory bodies, and user communities—wield considerable influence in shaping the architecture and functionalities of IoT devices. The stabilization phase is also marked by the solidification of alliances, as multiple stakeholders find common ground in promoting interoperability and data security. At this stage, deviations or disruptions become increasingly challenging, as any alteration would necessitate a reconfiguration of the established actor network. Nevertheless, stabilization is not an endpoint but a dynamic state; continuous engagement from all actors is essential for sustaining the network and accommodating emergent technologies and paradigms.

Network Expansion

Network expansion represents a critical juncture where the boundaries of the actor network extend beyond initial stakeholders to include an increasingly diverse set of actors. This can range from new user groups adopting smart home technologies to cities integrating IoT devices into public infrastructure. This phase is often marked by rapid innovation and proliferation of use cases, fueled by the stabilized core network. However, this expansion poses challenges in scalability, data management, and security, requiring active negotiation among existing and new actors to modify or adapt the initial protocols and norms. As the network grows, the actants multiply, adding layers of complexity but also the potential for enriching the ecosystem. The expansion phase is pivotal for the network's sustainability and adaptability, serving as a test for its resilience and capability to evolve.

Central Nodes

Within the Internet of Things landscape, certain actors—often non-human—emerge as Central Nodes that wield substantial influence over the network. These Central Nodes are usually high-capacity servers, data processing units, or even influential software algorithms that serve as crucial points for data routing, decision-making, and network maintenance. Through the lens of Actor-Network Theory, these Central Nodes are not mere relay stations but powerful actors that can shape network dynamics, facilitate or hinder connections, and significantly affect the network's resilience and functionality. For example, a cloud-based data center could be a Central Node that not only stores data but also employs algorithms to analyze it for predictive maintenance or anomaly detection. The failure or compromise of such a Central Node can have cascading impacts, affecting every actor—both human and non-human—linked to it. Thus, understanding the role and influence of Central Nodes is essential for comprehending the complex interplay of relationships that defines the IoT network.

Negotiations

In any Internet of Things (IoT) network, negotiations are an ongoing, intricate process that continually shapes the fabric of interconnections among various actors. Actor-network theory provides a useful framework to understand these negotiations, which often occur between actors—be it software algorithms negotiating access permissions, or human operators negotiating bandwidth allocation. For instance, a smart home system may involve negotiations between user preferences (a human actor) and energy-saving algorithms (a non-human actor). These negotiations define what is possible within the network and establish the conditions under which different actors can exert influence or undergo transformations. It is through these negotiations that alliances are formed, actors are enrolled, and network stability is either achieved or

compromised. The nuances of these negotiations can make or break the overall functionality and efficacy of an IoT system. Therefore, dissecting the negotiation processes is vital for understanding how the network evolves and how power dynamics are distributed among its constituents.

Data Privacy

In the intricate web of the Internet of Things, as explored through Actor-Network Theory, data privacy emerges as a highly contentious node where various actors' interests and roles often clash or realign. On one end, consumers are continuously negotiating for stringent data protection measures, actively acting as agents demanding clarity in how their data is collected, stored, and used. On the other end are manufacturers and software developers, who often view consumer data as invaluable for improving services and even monetizing it through targeted advertisements or third-party partnerships. Regulators, another set of human actors, step in to lay down policies and frameworks that dictate acceptable norms and limits within the network, often after heated negotiations and public discourse. However, data privacy is not merely a human-centric concern; non-human actors like encryption algorithms, firewalls, and cloud storage facilities play a pivotal role in shaping this dynamic. They either strengthen or weaken the network's ability to safeguard privacy depending on their efficiency and adaptability. In essence, data privacy in IoT is a negotiated space, reflecting both human and non-human actor interactions that continuously evolve and redefine the network's character and direction.

Accessibility

Accessibility within the Internet of Things (IoT) ecosystem, when viewed through the lens of Actor-Network Theory, is another critical junction where various actors negotiate, exert influence, and are in turn modified. Human actors like developers, consumers, and advocacy

groups are engaged in a continuous dialogue to make these technologies universally accessible. For instance, developers are influenced by regulations and market demand to create more inclusive devices and software. Meanwhile, advocacy groups and individual consumers push the accessibility agenda, acting as catalysts for change by lobbying for more user-friendly design or suing companies for non-compliance with existing regulations. However, the role of non-human actors in this discourse cannot be discounted. User interface design software, screen readers, and even voice-activated technologies are non-human actors that both shape and are shaped by these ongoing negotiations. These technologies either enable or hinder accessibility, thereby affecting the network dynamics. Additionally, standards and guidelines, often encoded into law, act as non-human actors influencing how human actors design and interact with IoT devices. Therefore, accessibility in the IoT space is a complex, negotiated reality shaped by interconnected human and non-human actors that co-evolve in response to multiple pressures and opportunities.

System Dynamics

System dynamics within the Internet of Things (IoT) manifest as a fluctuating interplay of influences, a complex web that Actor-Network Theory is particularly well-suited to dissect. On one hand, we have human actors such as policymakers, manufacturers, and end-users who generate demands and exert constraints on the IoT network. Policymakers set regulations that guide data use and device security. Manufacturers, striving for innovation and market share, push the envelope of what is technologically feasible, often shaping user expectations and norms in the process. End-users interact with IoT devices, adding a layer of complexity by introducing unpredictable usage patterns, which can lead to unplanned network stresses or novel functionalities. On the other hand, non-human actors, such as algorithms, data storage facilities,

and even the devices themselves, also play vital roles in shaping these dynamics. For example, a storage algorithm can prioritize data in a way that significantly impacts system performance and user experience. Similarly, device limitations can affect user interaction, forming a feedback loop that might influence future design. Therefore, system dynamics in the context of IoT are not merely a backdrop but an active, evolving landscape of multiple negotiations and transformations between human and non-human actors.

Future Implications

Examining the Internet of Things (IoT) through the lens of Actor-Network Theory illuminates not only its present complexities but also provides insights into its future implications. As IoT devices continue to proliferate and integrate into various facets of daily life—from smart homes to healthcare—future concerns like ethical considerations, data security, and environmental impact become increasingly critical. Human actors, such as policymakers and ethicists, will likely play a more pronounced role in shaping regulations that address these concerns. Meanwhile, non-human actors like advanced AI algorithms could redefine data privacy standards and energy-efficient chips could alter the environmental footprint of these devices. Further still, as the network expands, new actors—both human and non-human—will emerge, introducing new dynamics and alliances. For instance, community-based IoT networks might evolve, and with them, new local governance structures could be established. As IoT technologies advance, ongoing negotiations among these diverse actors will continually reshape the network, offering both transformative possibilities and cautionary lessons for a future increasingly dependent on interconnected devices.

Conclusion

The application of Actor-Network Theory (ANT) to the Internet of Things (IoT) provides a nuanced understanding of a rapidly evolving technological landscape. In this complex network, both human and non-human actors are interwoven in a fabric of relationships, negotiations, and alliances that shape the IoT's development, functionality, and societal impact. Human actors—ranging from policymakers and engineers to consumers—inject their goals, values, and expectations into the network. On the other side, non-human actors like IoT devices, algorithms, and data centers contribute autonomously to the network's dynamic, sometimes emerging as Central Nodes with significant influence. Through various stages of development, stabilization, and expansion, the IoT ecosystem evolves, solidifies alliances, and navigates challenges in scalability and data management.

The implications of this understanding are manifold. For policymakers and regulators, ANT offers a framework to consider not just the human elements but also the non-human components when formulating laws concerning data privacy, security, and accessibility. Manufacturers and software developers can leverage these insights to build devices and algorithms that are more aligned with consumer expectations and regulatory guidelines. In the realms of data security and privacy, recognizing the 'agency' of non-human actors like encryption algorithms and firewalls could pave the way for more robust protective measures.

In practical terms, the insights from this ANT perspective can be applied in diverse sectors, from smart homes and healthcare to industrial IoT applications. For example, community-based IoT networks could leverage local governance structures to manage the devices and the data they generate, making the network more resilient and adaptive to local needs. Businesses could better understand how to manage complex supply chain networks by

recognizing the role and influence of non-human actors like RFID (Radio Frequency ID) tags and logistics algorithms.

However, this approach is not without its limitations. ANT tends to level the playing field among actors, which might inadvertently dilute the accountability or ethical responsibility attributed mainly to human actors. For instance, considering a software algorithm as an 'actor' in a data breach scenario could obscure the responsibility of the human actors who created or deployed that algorithm. Moreover, the ANT framework often captures a snapshot of a continually evolving network, making it challenging to account for its temporal dynamics.

In summary, applying Actor-Network Theory to dissect the complexities of the Internet of Things provides a multifaceted lens to view its development, challenges, and implications. While not a panacea, ANT serves as a valuable analytical tool to help stakeholders better understand, navigate, and shape the intricate web of relationships that define the IoT landscape. As this network continues to expand, ANT can offer both transformative possibilities and cautionary lessons for a future increasingly dependent on interconnected devices.

References

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, *22*(2), 171–192. https://doi.org/10.1257/jep.22.2.171

Arif, S., Bakar, N. A., & Sidek, S. (2017). Actor-network theory (ANT) as an interpretive tool to understand the ... https://www.researchgate.net/profile/Sazelin-Arif/publication/326569510_Actor-network_theory_ANT_as_an_interpretative_tool_to_understand_the_use_of_online_technologies_A_review/links/5b56853eaca27217ffb6d394/Actor-network-theory-ANT-as-an-interpretative-tool-to-understand-the-use-of-online-technologies-A-review.pdf

Aziz Al Kabir, M., Elmedany, W., & Sharif, M. S. (2023). Securing IOT devices against emerging security threats: Challenges and mitigation techniques. *Journal of Cyber Security Technology*, 1–25. https://doi.org/10.1080/23742917.2023.2228053

Biberstein, P., & Rajesh, S. (n.d.). GDPR Case Study: Marriott International, Inc. - Brown University. https://cs.brown.edu/courses/csci2390/2021/assign/gdpr/pbiberst-srajesh1-mariott.pdf

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, *173*, 113–124. https://doi.org/10.1016/j.jpubeco.2019.02.001

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva papers on risk and insurance. Issues and practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Franklin, J. M., Howell, G., Boeckl, K., Lefkovitz, N., Nadeau, E., Shariati, B., Ajmo, J. G., Brown, C. J., Dog, S. E., Javar, F., Peck, M., & Sandlin, K. F. (2020). Mobile Device Security: Corporate-Owned Personally-Enabled (COPE). https://doi.org/10.6028/nist.sp.1800-21

Individual pleads guilty to participating in internet-of-things cyberattack in 2016. Office of Public Affairs | Individual Pleads Guilty to Participating in Internet-of-Things Cyberattack in 2016 | United States Department of Justice. (2020, December 9). https://www.justice.gov/opa/pr/individual-pleads-guilty-participating-internet-things-cyberattack-2016

Javaid, M., & Khan, I. H. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. Journal of oral biology and craniofacial research, 11(2), 209–214. https://doi.org/10.1016/j.jobcr.2021.01.015

Khare, S., & Totaro, M. (2019). Big Data in IoT. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). Kanpur, India. https://doi.org/10.1109/ICCCNT45670.2019.8944495

Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R., & Durumeric, Z. (2019, August 14). *All things considered: An analysis of {IOT} devices on home networks*. USENIX. https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak

ResearchGate. (n.d.). The facilitation of trust in automation: A qualitative study of behaviour and attitudes towards emerging technology in military culture [Scientific figure]. Retrieved November 2, 2023, from https://www.researchgate.net/

Ritchie, J. N. & A., & Jayanti, S. F.-T. and A. (2021, December 1). *Careful connections: Keeping the internet of things secure*. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure

Seuwou, P., Banissi, E., Ubakanma, G., Sharif, M. S., & Healey, A. (2016). Actor-network theory as a framework to analyse technology acceptance model's external variables: The case of autonomous vehicles. Global Security, Safety and Sustainability - The Security Challenges of the Connected World, 305–320. https://doi.org/10.1007/978-3-319-51064-4_24

Tatnall, A. (2019). Researching computers and education through actor-network theory. *Sustainable ICT, Education and Learning*, 78–88. https://doi.org/10.1007/978-3-030-28764-1_10

Xu, H., Yu, W., Griffith, D., & Golmie, N. (2018). A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. IEEE access : practical innovations, open solutions, 6, 10.1109/access.2018.2884906. https://doi.org/10.1109/access.2018.2884906