IoT Devices and Security: A Narrative Review

Robert C. Arnold

KORD Technologies, Inc.

KBR, Inc.

635 Discovery Dr.

Huntsville, AL 35806

Abstract

Since its inception, the internet of things (IoT) has expanded rapidly. Malicious actors have a vast attack surface at their disposal. In addition to cyberspace developing, cyber threats are becoming more sophisticated. IoT security flaws enable the spread of exploits. IoT device owners frequently lack the ability to reset passwords and/or download security fixes as security flaws crop up due to the global market's oversaturation with cheap and basic IoT devices. The ability to deliver devastating Distributed Denial of Service (DDOS) attacks on networks that can cause significant internet outages in targeted areas or industries is enabled by malicious actors commanding any one or a number of these unsecured IoT devices to create different levels of attacks. Cyberattacks keep getting bigger and more sophisticated as the IoT expands exponentially and suffers from a lack of security solutions. The biggest network security danger that administrators will have to deal with in the future is likely to be cyberattacks that use artificial intelligence (AI). These attacks would spread malicious code by making use of the entire range of IoT devices, including home, car, office, and medical ones. This could lead to a breach of the entire cyber domain. Network security must be protected from an infinite expansion of the attack surface.

Keywords: Internet of Things, Security, Past, Present, Future, Vulnerabilities

Introduction

This paper identified themes regarding how security is considered or implemented in the different stages of the Internet of Things (IoT), broken down into past, present, and future, based on a narrative literature review. Smartphones, wearable fitness trackers, laptops with remote access, cars, and even wearable or surgically implanted medical equipment are some examples of IoT devices. By understanding what IoT is, the different considerations of security, and the challenges that IoT faces, IoT devices can be designed to be more secure.

Malicious actors will design an attack to undermine the confidentiality, integrity, and availability (CIA) of desired data on a protected network by taking advantage of any network weakness. IoT has expanded the attack surface available to malevolent actors. The security expert is given levels of physical security via security-in-depth, which bad actors must breach to physically access sensitive infrastructure. These additional security layers prevent hostile actors from physically accessing key infrastructure, forcing them to make inventive efforts to install harmful code into a workspace where access is restricted. To help security professionals, create a risk management framework and provide a robust cyber security strategy in the presence of the IoT within the workspace, the goal of this study is to better understand how security is implemented in IoT devices and how security within IoT devices can help in the future. Congress has tried to define the IoT's extent and the threat it poses, but there is still no legislative structure in place to make it secure. Regarding IoT, affordability and usability have started to become more of a priority, rather than security (Rizvi, et al., 2018). Devices that do not prioritize security can potentially endanger not just human safety and security, but also national security. The IoT's development and security flaws give bad actors virtually unrestricted remote access to crucial infrastructure, which is a critical concern. IoT was first used in homes and offices, but with the development of smartphones, it is now connected to the internet outside of these two settings. The IoT already existed before the invention of smartphones (Farooq, et al., 2015), but it was only accessible in places like houses or offices that had a network connection. Apple unveiled the first-generation iPhone in late June 2007. The IoT expanded rapidly because of this release, due to the iPhone being the IoT pioneer (Rose, Eldridge, & Chapin, 2015). Because of the IoT's general lack of security, hostile actors can launch a variety of attacks. Criminal code could propagate to additional devices over a private network once malicious actors have gained control of one device, creating a network of computers infected by malware that is now under the control of a hostile actor, commonly known as a BOTNET. The IoT also exposes other cyber security flaws, such as distributed denial of service (DDoS) assaults facilitated by BOTNET. Malicious actors don't simply take advantage of flaws in system engineering designs; they also take use of gaps in well-intentioned rules and risk management strategies, which unintentionally widen the attack surface of private networks to the point where the malicious

intrusion is possible. IoT devices are no longer limited to the home or office thanks to mobile access to the internet. Instead, the IoT is present in all marketing forms, including automobiles, wearable fitness trackers and sensors, implanted surgical gadgets, appliances, and even apparel. While there were 6.8 billion people on the planet, consumer demand increased IoT device numbers to 12.5 billion because of further integration of the IoT into other daily activities. Evans predicted that by 2020, there will be 7.6 billion people on the earth and 50 billion IoT devices in operation, or 6.58 IoT devices per person (Evans, 2011). There were 50 billion IoT devices on the earth in 2020, producing 4.4 zettabytes of data (Gold, 2020).

According to Beale and Berris (2017), the biggest danger posed by the IoT to personal and national security is the exception that is made to c rules. While communicating with service providers and other networked devices is the purpose of networked devices, the IoT poses a serious insider danger to all networks. Users are restricted to the pathetic factory security settings that come pre-installed on their networked devices. Many IoT devices have hardwired firmware and passwords, preventing users from using simple security or privacy features like updating firmware or changing passwords (Beale & Berris, 2017). Erboz (2017) asserts that the advent of the IoT, together with cyber-physical systems, on-demand availability of computer system resources (cloud computing), and cognitive computing, has ushered in the fourth industrial revolution (4IR). If the IoT is expanding without much attention paid to security, previously unanticipated security flaws will continue to emerge exponentially. IoT was identified at the Massachusetts Institute of Technology (MIT) in 1999 (Kevin Ashton, n.d.), but it has since spread globally due to the widespread use of IoT devices both inside and outside of the home and workplace. Each IoT device presents a potential security risk to every user online. Over the past two decades, the attack surface has significantly increased due to the exponential proliferation of IoT devices in homes and offices. At first look, the future seems incomprehensible, but this analysis will offer a qualitative forecast of the common themes across multiple articles. IoT is the low-hanging fruit for both cyber security experts and dangerous attackers (F-Secure, 2018). Convenience over security was prioritized in the design of IoT devices, which might lead to serious vulnerabilities and prevent owners from updating security measures, providing hackers with a bounty of easy targets. Users bringing IoT devices into an area where they represent the highest security concerns unintentionally create significant insider hazards as a result. These well-known design flaws can be used by malicious actors as network attack vectors, as much as users' inability to upgrade firmware or change passwords multiplies attack surfaces. It was predicted by Evan in 2011 that more than 50 billion IoT gadgets would be a part of daily life as wearable, drivable, or linked devices within our living environments at home by 2020, the Federal Trade Commission made a similar prediction in 2017. (114th Congress, 2016) This forecast has come true because of the emergence of "smart homes & offices," IoT-enabled "infotainment centers," and modern automobiles (Paganini, 2021).

This initial research phase will examine the history of the Internet of Things, from its inception to its current prevalence in daily commuting, office, and home life. The next stage of this study will involve understanding the IoT's future and exploring what security experts can do to defend against the IoT's constantly expanding attack surface. An ever-expanding attack vector for bad actors is the IoT.

Problem Statement

Many people use the IoT in their daily lives and in office settings. This use includes wearable gadgets like the Apple iWatch, Fitbit, and other similar devices as well as peripheral computer devices.

Through the execution of promptness tasks, which are traditionally carried out by people, AI may be the force multiplier that bad actors aim to exploit. The release of this "tireless monster" might be so overwhelming that security specialists would lose all hope. The problem is that IoT devices are being developed and implemented without consideration for security. This problem is made worse by the fact that some implantable or wearable devices with wireless connections to the cyber domain could transmit harmful code. With the introduction of IoT devices in areas that are close to sensitive or classified systems

or networks, serious vulnerabilities could emerge. These implantable and wearable gadgets could be dangerous for personal safety as well as national security. The dual usage of their well-intentioned work could unintentionally have terrible implications, thus researchers developing AI should be very careful about creating a dangerous Frankenstein monster. AI-enabled IoT may be a nightmare scenario, but it may also be the key to solving its issues. By implementing AI that is security-focused, the IoT might serve as a delivery system for benevolent AI to be distributed throughout the cyber domain to find and remove bad code and lessen the intentions of hostile actors (Brundage, et al., 2018).

Purpose

The purpose of this study is to examine how the IoT has changed the security posture over time, by conducting a comparative analysis with key articles on the different security implications and challenges that the IoT has faced. The IoT's future and its impact on the security of private and classified networks will be predicted by further investigation, as well as the awareness that individuals have of their devices and the security configured on them.

Research Questions

Consistent with the purpose of the study, the following research questions are answered:

RQ1: How can malicious actors infiltrate networks and sensitive and confidential information systems using IoT as an attack vector?

RQ2: In what ways can IoT increase the security of current networks?

Review of the Literature

What is IoT?

We must precisely define the IoT before we begin any work to investigate its past, examine its present, or do any type of analysis regarding its future. IoT is a networked collection of connected gadgets. Any gadget with an IP address, identification, and internet connection nowadays is part of the IoT. (Gazis, 2021) IoT refers to an expanding network of electronic devices that don't typically match the definition of a computer but instead communicate with one another over the internet to carry out certain tasks. IoT growth has been exponential since its inception. The heterogeneity of the IoT is the first challenge it has encountered in the past, present, and future. To handle data, each of these various systems or devices uses circuitry and protocols that are distinct from the others (Butun, Osterberg, & Song, 2020). IoT is the next development of the internet, according to a white paper written by Dave Evans in 2011 titled "The Internet of Things: How the Next Evolution of the Internet is Changing Everything." IoT gadgets can be found in our homes, workplaces, retail establishments, and even automobiles. 500 million devices were online in 2003 when there were roughly 6.3 billion people on the planet. The invention of smartphones provided these devices with access to network connectivity outside of the house or workplace, which served as a crucial catalyst for the IoT's rapid expansion. With a global population of 6.8 billion people in 2010, connected IoT devices had multiplied to 12.5 billion thanks to the smartphone. In 2006, more Internet of Things (IoT) devices existed than people on Earth. Evans predicted that there will be 6.58 billion people and 50 billion IoT devices on the earth by 2020. (Evans, 2011) Evans' estimate of 50 billion IoT devices by 2020 was not the only one; the DHS Cybersecurity Strategy predicted that by 2020 there would be 20 billion networked devices connected to the cyber domain. (DHS Cybersecurity Strategy | Homeland Security, n.d.)

Security experts' capacity to respond to the escalating security concerns posed by this massive attack surface has been outpaced by the IoT's accelerating growth. Vehicles equipped with IoT contain security flaws that have been exploited by bad parties to endanger driver security (Beale & Berris, 2017). By utilizing networked thermostats in aquariums to access casino networks, malicious actors have

jeopardized the privacy of important data (Wei, 2018). IoT devices utilized in the medical sector have security flaws that can be exploited to attack networks in the healthcare sector. (Shpachuk, 2022)

The Past of IoT

With the advent of the internet and the creation of the first manufactured domain, the third industrial revolution began around 1980. Erboz asserts that the IoT emerged in the late 1990s as the start of the 4IR (Erboz, 2017). Like the space realm, navigating the cyber domain requires an interface device. Cyber domain users require a networked computer in place of rockets and spacecraft to access the cyber domain. Early space exploration gave humanity the chance to place satellites into orbit that were used for a variety of reasons. Some are there to convey communications information around the globe, while others are there to monitor the weather. Some exist to keep an eye on global activity and alert governments to any hostile actions by their enemies from Earth's orbit. Unsecured IoT devices could function as satellites in the space realm, able to conduct remote monitoring operations from a low earth orbit. Instead, we have IoT gadgets in our cars, homes, and our bodies. In addition to providing malevolent actors with a platform to covertly watch individuals, this flood of satellites in cyberspace also offers offensive potential. A nation's ability to communicate, conduct financial transactions, navigate to unfamiliar locations, or engage in any other activity that requires transitional/receipt of data in a two-way handshake on the cyber domain IoT devices could be completely compromised by activating a botnet of billions of IoT devices in a geographic area.

The IoT has ushered in the 4IR, but with its ease also come potential security flaws that could exist with any gadget whose comfort of use takes precedence over security (Erboz, 2017). Numerous claims have been made by security experts about the flaws in the ever-growing number of networked gadgets. By preventing users from updating security protocols on these devices, unchangeable factory settings on the devices allow for security vulnerabilities that are exponentially made worse. The introduction of smartphones in 2007, which made it possible for IoT devices to maintain network connections while in motion, caused the IoT industry to grow. By enabling remote access to sensors, transceivers, and other equipment in nearby or distant locations, these networked devices aimed to reduce the labor intensity for operators. IoT devices started using sensors as extra input devices in or about 2013, enabling hostile actors to use them for technical information gathering. (Simon IoT, 2022)

Current Usage of IoT

The IoT is used differently than it is intended to be used. The purpose of networked thermostats, wearable fitness trackers, surgically implanted medical sensors, smartphone-enabled kids' toys, 5^{th}-generation cellular networked cars, and/or Wi-Fi and Bluetooth-enabled peripheral computer equipment was to serve as labor-saving tools. Unfortunately, user demands for affordability and convenience of use have led to an ever-growing security risk that has never previously been experienced by mankind (Beale, & Berris, 2017). According to Representative Anna Ashoo's speech to the 116th Congress in 2016, 6.4 billion connected IoT devices were in use globally. The world's population was just under 7 billion people in 2016. According to Ashoo's claim, there is more than one gadget for every person on the earth, which would place the IoT. That figure, 2.3 billion, according to Statista, suggests that people outnumber IoT devices by a factor of nearly three to one. Even while that estimate was incorrect by more than four billion, it still presents a dire situation (Statista, 2021). Because of these skewed numbers, an additional study using a larger IoT statistics data set is required. When Dave Evans predicted the IoT's future in 2011, he had access to only roughly 4 years' worth of data, which was insufficient at the time to make an accurate forecast. Using a variety of analytical strategies, we can now identify trends and make much more precise predictions thanks to the benefit of more than fifteen years' worth of data. When the results are compared, the analyst is given a much smaller confidence interval around the upper and lower predictive thresholds. The analyst will receive a considerably more precise prognosis thanks to the smaller confidence interval.

Future Usage of IoT

There will undoubtedly be rapid growth in the IoT in the future. According to Moore's law, the size of a transistor on a circuit doubles every two years. A similar predictive technique was used in a Chinese study that showed the internet doubled in size every 5.32 years (Zhang et al., 2008). With this information, it is quite probable to estimate how the Internet and the Internet of Things will grow over the coming years. Although the "size" of the internet cannot be quantified, the number of connected devices is increasing rapidly in both quantity and complexity over time. Predictions are exceedingly challenging because accurate data on the state of the IoT is hard to come by. To create a forecast of what the IoT might look like in the following year, Dave Evans evaluated the IoT in 2011 using the scant data that was available at the time. Using data spanning eight years, Evans estimated that the number of IoT devices exceeded that of the world's population in or around 2007, which was close to the time the smartphone hit the market and enabled the IoT to grow rapidly. With a global population of 7.6 billion, Evans anticipated that the IoT would reach 50 billion devices by 2020, or 6.5 IoT devices for every person on the earth (Evans, 2011).

During the second session of the Joint Hearing before the Subcommittee on Communications and Technology and the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce House of Representatives 114th Congress gathered to discuss the status of the IoT in the present tense and make a prediction of its future. During her address to the 114th Congress, Representative Anna Eshoo, of California, stated there were 6.4 billion IoT devices existing worldwide in 2016. According to Statista (2021), this was a dramatic under-calculation, as their numbers stated that there were closer to 15 billion IoT devices worldwide in 2016. In a later projection, Representative Eshoo predicted that 20 billion IoT devices would be online by 2020. Representative Marsha Blackburn of Tennessee predicted the IoT would have 3.4 billion linked devices by 2020 in the same speech to the 114th Congress. Statista estimates that there were closer to 15 million IoT devices in use in 2016 and that there will be 30 billion in use in 2020. (Statista, 2021) I was inspired to create my own data pool because state officials testifying before Congress in 2016 found it challenging to present consistent statistics to define the IoT. (114 Congress, 2016) Cyberattacks made possible by artificial intelligence (AI) could have unthinkable repercussions (Brundage, et al., 2018). AI-enabled malicious code might reproduce and evolve to disrupt the IoT so quickly that it could overwhelm even the most astute investigators and security experts if it were unleashed into the wild of the cyber realm (Kaloudi & Li, 2022). By duplicating and rerouting itself through an inconceivable number of servers via the network of networked IoT, AI might further complicate attribution by avoiding capture without the need for command and control (Clark & Landau, 2011).

Method

Selected articles involving the past, present, and future of IoT devices, involving the different considerations and challenges of security, will be reviewed, and then assessed with a narrative review. Using Delve, a tool designed to help with organizing a thematic analysis, I imported each of the different applicable transcripts from the key articles. Once patterns are identified, individual and related codes will be developed showing relationships within the transcripts. Lastly, major themes are developed to group each of the related codes. It is anticipated that most articles will be identified based on forward and backward citation searching from the key articles found. Date range restrictions for articles will be applied. All articles chosen must be from the last 15 to 20 years. Also, relevant articles with empirical data or literature reviews will also be identified by scanning titles and abstracts from searching in Galileo, Google Scholar, and IACIS journals with the terms Internet of Things, IoT Devices, IoT, and security. Inclusion criteria will be that the abstract text includes relevant content, as judged by this researcher.

Data Analysis

A thematic analysis was utilized to show the relevance and comparison of the data (Creswell & Tashakkori, 2007). Creswell (2007) defines that this analytic procedure entails finding, selecting,

evaluating, comparing, and synthesizing data contained in the researched articles, then organizing the data into major themes and categories, including common codes.

In total, 14 key articles and 50 on-topic articles were used in the narrative review. As displayed in Table 1, the contributions from the key articles were identified and grouped into three emerging themes and a set that provided theoretical foundations for all themes. The three themes that emerged were: (1) The beginning of IoT devices and the consideration of security, (2) current IoT devices, the security that is being utilized and how they are being implemented, and (3) the future of IoT devices, the challenges and how security needs to be acknowledged.

Results

Theme 1: The Beginning of IoT Devices and the Consideration of Security

For the first theme, researchers documented the fundamentals of what IoT is, how it is being used, and the different considerations of security. Three studies are described regarding this theme.

TABLE 1: Theme, Reference, and Main Contribution of Key Articles

Theme	Authors (Year)	Main Contribution
1	Madakam, Ramaswamy, and Tripathi (2015)	Literature review includes identifying the basic concept and idea of IoT being based on RFID
1	Gharami, Prabadevi, and Bhimnath (2019)	Semantic analysis on the past, present, and future of IoT and the considerations of security
1	Mattern and Floerkemeier (2010)	Empirical findings on the vision of IoT
2	Deep, Zheng, Jolfaei, Yu, Ostovari, and Bashir (2019)	Survey on how security is being implemented across the platform of IoT devices
2	Nurse, Creese, and De Roure (2018)	Challenges of assessment of risk in IoT systems
2	Kirtley and Memmel (2018)	Implementation and challenges of privacy and security in IoT
2	Blythe, Johnson, and Manning (2020)	Study on if consumers are willing to pay for more security on IoT devices
2	Roman, Zhou, and Lopez (2013)	Empirical findings on the challenges of security in IoT
2	Leloglu (2017)	Review of security concerns in IoT
3	Rose, Eldridge, and Chapin (2015)	Empirical findings about how security is a pressing challenge and the questions related to IoT
3	Shuo-Yan Chou (2019)	Empirical findings on the future of the 4IR and the security challenges
3	Jindal, Jamar, and Churi (2018)	Future challenges of IoT; with a focus on security
3	Liu, Zhao, Li, Zhang, and Trappe (2017)	Future internet architecture for IoT
3	Patel, Patel, and Scholar (2016)	Application and future challenges of IoT

Note. IoT = internet of things; RFID = radio frequency identification; 4IR = Fourth Industrial Revolution; 1 = the beginning of IoT devices and the consideration of security; 2 = current IoT devices and the security being utilized; 3 = the future of IoT devices and the acknowledgment of security.

In the first study (Madakam et al., 2015), IoT was identified as being a technological revolution that represents the future of computing and communications. The growth of the IoT is dependent on rapid technological advancement in several key areas, including nanotechnology and wireless sensors. The study

also emphasizes the fact that IoT aspires to integrate everything in our world under a single infrastructure, allowing us control over the things around us and keeping us updated on their status. The concept of IoT was based on members of the RFID community, who served as the original inspiration for the IoT when they discussed the idea of learning more about a tagged device by looking up a website address or database record that matches to a certain RFID or Near Field Communication technology.

In the second study, a semantic analysis was conducted by Gharami, et al. (2019) discussing how IoT is seen as things interconnected either through some wired or wireless medium hovering around wide area network protocol, sensors, and technologies. The study also described how the IoT applications and predictions cover a wide range of fields, including those related to health, upkeep, services, public sector implementation, social applications, medical aids, healthcare, elderly assistance, crude energy management, traffic management, smart cities, smart home appliances, smart watches, smart lifestyle, smart grids, smart telecommunications, smart agriculture, and many others that make life simpler and less chaotic. The authors also discussed how security was considered in the development of IoT, by conducting a small survey study that showed results on how security in interfaces was hindered, encryption was not found, methods of secure passwords were not followed, and most dealt with privacy concerns. A third study (Mattern & Floerkemeier, 2010) discusses the vision, different challenges, potential usage scenarios, and the technological building blocks of IoT, with a specific focus on how IoT has spread rapidly over the years, by being included in book titles, conferences, and other research.

Theme 2: Current IoT Devices, the Security that is Being Utilized and How They Are Being Implemented

Across several of the studies, different types of research were conducted to see how security was being utilized and implemented across the platform of IoT devices, where professionals found areas of weakness within security. According to one study (Deep, Zheng, Jolfaei, Yu, Ostovari, & Bashir, 2019), the IoT is a cutting-edge paradigm that not only enables widespread Internet connectivity for a huge number of objects but also offers a method for remote control of such things. The Internet of Things is omnipresent and practically a need in our daily lives. Users' private information is frequently collected by these linked gadgets and stored online. In the modern era, data security is a major worry. The privacy and security concerns that arise because of the proliferation of connected devices must be urgently addressed. The security and privacy of consumers could be jeopardized by threats to IoT implementations and devices, which could hinder their practical deployment. This specific study also found that to secure the IoT, there are still unresolved problems and difficulties that must be overcome. As a result, IoT systems have security flaws and are open to several assaults. A great example showing the areas of weakness in the IoT layers is provided below:

IoT Layer	**Security Issues / Attacks**	**Security Parameters**
Application	data access and security authentication issues, data protection and recovery problems, spear-phishing attack, software vulnerabilities, attacks on reliability, and clone attack	Data Privacy, Access Control
Middleware	making intelligent decisions processing huge data, malicious-code attacks, multi-party authentication, handling suspicious information	Integrity, Confidentiality
Network	cluster security problems, DoS attacks, spoofed, altered, or replayed routing information	Authentication, Integrity
Perception	node capture, fake node, mass node authentication, cryptographic algorithm, and key management mechanism	Integrity, Authentication, Confidentiality

In the second study, the challenges of current risk assessments were addressed, particularly with IoT, on the need for new approaches to assessing risk (Nurse, Creese, & De Roure, 2018). The problem with IoT and similar connected systems is those extremely dynamic systems may render useless the periodic and knowledge-intensive processes used by current risk assessment methodologies. IoT systems are simply

too quick-moving for such an aggressive strategy. The possible variability of connections, the possibility that some may grow to be highly (or less) trusted, and the potential impact on the risk management practices that surround them, would all need to be considered in new approaches.

A third study (Kirtley & Memmel, 2018) found that IoT observers and stakeholders have expressed privacy and security issues with IoT devices for a few years. IoT devices' direct collection of sensitive data, such as financial account numbers, health data, exact geolocation, and other information, is the main privacy worry. The authors also found that the vulnerability of IoT devices to cyberattacks, like the May 2017 WannaCry attack and the October 2016 DDoS attacks that targeted the IoT, is the main security worry. The five sectors in which IoT technology has been deployed and used were one of the article's key points. The first of these five categories are linked automobiles, followed by consumer IoT, health IoT and medical devices, smart buildings, and smart manufacturing. The correct implementation of security inside consumer IoT software, firmware, and hardware is frequently neglected and disregarded priority, as was the case with each sector that highlighted distinct security concerns. According to the article, consumers "may not be aware of the far-reaching security vulnerabilities introduced by something as innocuous as connecting a smart LED bulb to the[ir] home network." (Kirtley & Memmel, 2018) A fourth study provides details on a study that was conducted to see if consumers are willing to pay additional money for a more secure IoT device. The results reflected that consumers would rather pay more than be open to vulnerable devices. The study also explained how most IoT devices are developed without security in mind, resulting in IoT products having flaws, including smart toys that let hackers listen in on children's talks, smart locks that let people's homes be broken into without their permission, and smart TVs that could facilitate the transmission of false information. These (and other) IoT devices have vulnerabilities that can be used by cybercriminals to access, delete, and damage customer data and hardware, as well as support cybercrimes. With the help of experts, horizon scanning research has identified a wide range of potential crimes that could be committed using consumer IoT, including terrorism, sex crimes, and blackmail.

In a fifth study, Roman and colleagues (2013) identified how the concept of IoT has evolved over time, while also giving a detailed examination of the characteristics and security issues associated with IoT's dispersed approach to determine where it fits into the larger scheme of the future internet. The study concluded with information on how numerous problems need to be resolved, including ensuring interoperability, developing a business plan, and controlling entity authentication and authorization. A sixth study (Leloglu, 2017) provides findings on how IoT envisions a technologically optimistic future in which any device can collaborate intelligently with another object at any time or any place. However, even if it has made significant progress, there are still concerns about the security concepts of its utilization, which are typically regarded as a top priority in the design of IoT architectures. Leloglu also emphasizes the fact that there are several problems with its widespread adoption, and it doesn't appear that it will ever be a technology that is used in the near future without providing pertinent remedies for the recently given challenges.

Theme 3: The Future of IoT Devices, the Challenges and How Security Needs to be Acknowledged

With this theme, what emerged was the future of IoT and the different security challenges that needed to be addressed. The IoT raises substantial hurdles that could prevent its potential benefits from being realized, according to one study (Rose, Eldridge, & Chapin, 2015). Public interest has already been piqued by attention-grabbing news about the hacking of Internet-connected gadgets, surveillance issues, and privacy problems. In addition to additional policy, legal, and development concerns, there are also technical obstacles to overcome. One of the major IoT problem areas is also discussed in this study, and it is studied to explore some of the technology's most urgent problems and issues. Although security issues are not new in the context of information technology, many IoT implementations' characteristics create new and distinct security concerns. It must be a top priority to address these issues and guarantee security in IoT goods and services. Particularly as this technology grows more prevalent and interwoven into our daily lives, users must have confidence that IoT devices and related data services are secure from threats. Inadequately protected data streams on IoT devices and services can act as potential ports of entry for cyberattacks and expose user data to theft. Because IoT devices are interconnected, every unsecured device that is connected to the Internet can influence the global security and resilience of the Internet. Other factors

include the widespread deployment of uniform IoT devices, the capability of some devices to automatically link to other devices, and the possibility that these devices may be used in unsafe locations all contribute to the difficulty of this problem. As a matter of principle, creators, and users of IoT systems and devices have a duty to guarantee that their work does not put users and the Internet at risk. To create efficient and acceptable solutions to IoT security difficulties that are well-suited to the scope and complexity of the issues, a collaborative approach to security will be required.

In a second study, Chou (2019) discusses how IoT capabilities can be combined with AI and blockchain capabilities to create synergy between the three types of technology. In addition to its progressive expansion and adoption, IoT integration has demonstrated outstanding synergy. IoT systems can supply a wealth of real-world data to increase the capabilities of AI. The impact of the 4IR will grow because of these improved, collaborative, and reliable IoT versions. The author also emphasizes the fact that IoT can be considered as a paradigm transfer to other sectors and provides details on the realization that smart factories and smart production is synonymous with achieving Industry 4.0 status in the industrial sector. Like this, IoT can be used to achieve the digital transformation of physical operations across all other sectors, including health, education, commerce, finance, tourism, transportation, construction, and agriculture, with considerable advantages. Thus, the manufacturing sector is not the only one that has been impacted by the 4IR. However, as a result throughout the 4IR, security and privacy issues in digital systems will become even more crucial. There will be many more potential breach points if numerous system components only have minimal degrees of protection implemented, which will make connected systems more vulnerable and make it more challenging to secure their operation. To guarantee the legitimacy of the users and the system's data, further cybersecurity precautions must be performed. Interestingly, this criterion can be met using technologies like blockchain, where it is possible to confirm both the sender's identity and the authenticity of the stored or transmitted data. Furthermore, widespread surveillance is no longer just confined to the internet. The idea of the all-seeing eye is becoming a reality thanks to the pervasive presence of proactive, and occasionally intrusive, cameras and other sensors. Even when consumers are not actively using functionalities that require such information, businesses have been gathering location and trip data through personal mobile phones. One can observe people's travel destinations, activities, meals, attire, doctor visits, and a variety of other such things. More comprehensive and potentially damaging physical activity data can be gathered, which might make it harder for some people to receive assistance or find employment. Through IoT, criminals may remotely access and control several sites at once, posing a considerably higher threat to physical infrastructure.

The third study (Jindal, Jamar, & Churi, 2018) presents the future challenges of IoT, specifically focusing on the technical security challenge. The authors provide details on how major security risks caused by IoT have caught the attention of numerous governmental and private sector enterprises worldwide. A broader platform for system intrusion will be made available to attackers by the addition of such a vast number of additional hubs to the systems and the web, especially given that many already suffer from security flaws. Indications suggested that the malware deployed a limitless number of IoT devices, such as smart home appliances and closed-circuit cameras, employed in basic applications, against their own servers. The manner in that IoT becomes integrated into our lives will lead to a further crucial development in security. A fourth study (Liu, Zhao, Li, Zhang, & Trappe, 2017) found that security is a major concern because most of the acquired data will be made available to a large and frequently unidentified audience when connecting numerous standalone IoT gadgets through the Internet. Unfortunately, many conventional security techniques cannot be used to secure IoT systems due to the inherent capability limitations of low-end IoT devices, which make up the majority of IoT end hosts. This leaves open the possibility of attacks and exploits targeted at both IoT services and the wider Internet. The authors suggested developing a lightweight keying protocol, for the future IoT, to establish trust between an IoT device and the IoT-NRS after developing an IoT name resolution service (IoT-NRS) as a fundamental element of the middleware layer. As a result of this design, local IoT systems are integrated into the global Internet through a design that maintains usability, interoperability, and security protection.

In a fifth and final study, Patel, and colleagues (2016) observed the key future challenges and implications for IoT, that need to be addressed before mass adoption will occur. The findings revealed in detail each of the different future challenges that will need to be addressed. These challenges are privacy and security, cost versus usability, interoperability, data management, and device-level energy issues.

Discussion

The narrative review confirms that even though IoT has made significant technological advances, security challenges do exist within the current architecture. In addition, the review provided positive workarounds on exactly what the challenges are for IoT, which provided insights on how to improve IoT for the future. This review extends the current understanding of the past, present, and future of IoT devices and thus has implications for improving and increasing security and overcoming challenges, and future research. Also, in this section, the answers to the research questions will be discussed.

Implications for Improving Security

Based on this review, the weaknesses in security related to IoT devices have the potential to negatively impact each of its users, by having openings for malicious actors to infiltrate. Using the data collected in the narrative review, I was able to conclude that because of several properties of the underlying technology, threats against IoT systems and devices translate to greater security risks. Answering research question one, the review also provided data on how IoT devices can be used by malicious actors to conduct an attack. IoT environments are useful and effective because of these qualities, but threat actors may take advantage of them. Due to this advantage, malicious actors have an open attack surface to pose a big threat to networks and different types of information, sensitive or confidential. These attack surface areas can be broken down into devices, communication channels, and applications and software. Devices may serve as the main method of attack initiation. Memory, firmware, the physical interface, the web interface, and network services are examples of components where vulnerabilities may exist in a device. Attackers may also benefit from outdated components, insecure update systems, and insecure default settings. Attacks may come through the channels that link different IoT components together. IoT system protocols may have security flaws that have an impact on the entire system. IoT systems are also vulnerable to well-known network assaults such as spoofing and denial of service (DoS). Lastly, systems can become compromised because of flaws in IoT device software and online apps. For instance, malicious firmware upgrades or user passwords can be stolen through web applications. To support the findings, the Silex malware attack that occurred in 2019 (Silex Malware, 2022) proved that IoT devices are susceptible to attacks. The Silex malware attack infiltrated hundreds of IoT devices and "bricked" them, rendering them functionally equivalent to a brick by rendering them useless. The devices' storage was damaged, their network configurations were wiped, and their firewalls were removed during this attack, which was launched by a 14-year-old hacker. Ultimately, the devices were stopped. IoT devices with known or crackable credentials that ran Linux or Unix were especially targeted by hackers. Most device owners found the manual firmware reinstallation process to be too difficult, but it was necessary for victims to recover their IoT devices.

Implications for Increasing Security

This review also sheds light on ways IoT can increase the security of current networks, providing the answer to research question two. The process of protecting these devices and ensuring they do not bring dangers into a network is known as IoT security. At some point, an attack is likely to occur on anything connected to the Internet. Attackers may use several techniques, such as credential theft and vulnerability exploits, to attempt to remotely compromise IoT devices. However, IoT devices generate a lot of data, such as logs and analytics, which can be tracked and analyzed to not only track performance but also proactively find and fix security flaws. Using the appropriate tools and best practices will help stop the next major attack. To increase security using IoT devices, protection solutions with an AI and ML focus need to be updated technologically. The minimum human engagement required by AI and ML will reduce downtime and improve organizational performance in spotting anomalous activity. The AI protection solution uses datasets, aberrant behavior detection, and security pattern analysis to provide free mistake detection. It should receive information from all corporate endpoints and run a statistical algorithm to enable logical

decision-making to evaluate the results. Early danger identification enables the early avoidance of protection concerns thanks to predictive analytics and excellent risk management. Due to this, providers of security measures are being compelled to switch from traditional to ML-based integrated technological solutions.

Conclusion

This narrative review concludes by illuminating the wide body of knowledge pertaining to the massive attack surface of IoT devices and how they may disrupt infrastructure around the world in terms of personal, business, and governmental use of the cyber domain. Despite the tremendous advancements in technology, inventions, and connectivity, IoT manufacturers are looking for new markets to grow their businesses. The next generation of connectivity companies is looking for technology that can integrate many participants with the internet infrastructure. Collaboration between cybersecurity businesses and AI-based service providers is necessary to develop new technologies and take advantage of market opportunities. The AI-driven IoT security market is fragmented, with big global technology giants and several startups focusing on AI and IoT. The market is anticipated to slowly consolidate once existing multinational goliaths begin aggressively acquiring and working with AI-based breakthroughs.

Developing a security standard for IoT devices is merely the first step in creating a more secure cyber domain. If enough compromised IoT devices connect to a botnet based on the same malicious code, the whole of the internet could be compromised and become useless. This would result in a failure of the 16 critical infrastructure sectors in the United States alone. This would also be catastrophic for developing nations that are dependent on the cyber domain for all communications. The IoT is the greatest insider threat to private networks. When malicious actors use wearable or implanted IoT devices to deliver malicious code, the user may be completely blind to the fact. Malicious actors will continue to seek ways to compromise classified and proprietary networks using whatever tools are available to them. The trouble is that there is insufficient security in IoT devices to ensure their safe use in areas where devices are traditionally forbidden.

Cyberattack complexity is also projected to increase as a result of AI that can weaponize the IoT. No matter how many IoT devices we have in the future, how we secure them now will be essential to creating healthier cyber hygiene habits later. A qualitative estimate of the current number of IoT devices is technically achievable, and a forecast of the number in the future is measurable with the sufficient study of a large enough data set. The security posture of the cyber domain as well as the personal security of users of IoT devices will be significantly impacted by improved security features of IoT devices.

Limitations

The review has substantial limitations as a general study because there was so much information available on IoT devices. More of the IoT and its impact on security falls within the scope of the study as the attack surface of the IoT and the effects of its devices on network security are reduced. Additionally, rather than allowing each user to implement security on their own device, doing a quantitative review to determine the level of awareness people have about their IoT devices' security would demonstrate if these devices needed to be built with security already applied.

Recommendations for Future Research

This research identified both positive and negative data for IoT devices and how security is considered. At this time, it is not clear how aware most individuals are about the lack of security that is missing from their IoT devices, which can potentially have a negative impact on the data or information that are using. Future research can clarify the awareness that users have about their IoT devices, which can provide results on if users are aware or unaware if their IoT devices have security mechanisms configured.

In the future, it is likely that there will continue to be attack vectors on IoT devices, due to a lack of security. However, this attack vector can be shrunk if users of these IoT devices are more aware and provide additional security configuration on their IoT devices. One predicted quantitative research, such as regression analysis, can help show how aware users are if their IoT devices are secure, as a dependent variable, and implement influencers (age, gender, etc.) as independent variables.

References

Ashton, K. (n.d.) *Kevin Ashton invents the term "The internet of things"*. Kevin Ashton Invents the Term "The Internet of Things" : History of Information. https://www.historyofinformation.com/detail.php?id=3411

Beale, S. & Berres, P. (2017). Hacking the Internet of Things: Vulnerabilities, Dangers, And Legal Responses. *DUKE LAW & TECHNOLOGY REVIEW*, *16*(1), 161–204. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1319&context=dltr

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science, 9(1), 1–9. https://doi.org/10.1186/s40163-019-0110-3

Brundage, B., Shahar, A., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Roff, H., Dafoe, A., Scharrel, P., Zeitzoff, T., Eckersley, B., Anderson, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S., Beard, S., Belfield, H., Page, M., Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Arxiv.Org. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/comst.2019.2953364

Clark, D., & Landau, S. (2011). *Untangling Attribution*. Harvard National Security Journal. https://harvardnsj.org/2011/03/untangling-attribution-2/

Creswell, J. W., & Tashakkori, A. (2007). Differing perspectives on mixed methods research. Journal of mixed methods research, 1(4), 303-308.

Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Bashir, A. K. (2019). A survey of security and privacy issues in the Internet of Things from the layered context.

Department of Justice. (2017, January 17). *Title III Regulation Supplement: Nondiscrimination on the Basis of Disability by Public Accommodations and in Commercial Facilities*. Www.Ada.Gov. https://www.ada.gov/regs2010/titleIII_2010/title_iii_reg_update.pdf

DHS Cybersecurity Strategy | Homeland Security. (n.d.). Retrieved October 18, 2022, from https://www.dhs.gov/publication/dhs-cybersecurity-strategy

Erboz, Gizem. (2017). How To Define Industry 4.0: Main Pillars Of Industry 4.0. https://www.researchgate.net/publication/326557388_How_To_Define_Industry_40_Main_Pillars_Of_Industry_40

Evans, D. (2011, April). *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*. Cisco Internet Business Solutions Group (IBSG). https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

F-Secure. (2018). *IoT Threat Landscape: Old Hacks, New Devices*. Blog-Assets.f-Secure.Com. https://blog-assets.f-secure.com/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). International journal of computer applications, 113(1), 1-7.

Leloglu, E. (2017), "A Review of Security Concerns in Internet of Things", *Journal of Computer and Communications*, 5, 121-136. doi: 10.4236/jcc.2017.51010

Gazis, A. (2021). What is IoT? The Internet of Things explained. *Academia Letters*. https://doi.org/10.20935/al1003

Gharami, S., Prabadevi, B., & Bhimnath, A. (2019). Semantic analysis-internet of things, study of past, present and future of IoT. Electronic Government, an International Journal, 15(2), 144-165.

Gold, J. (2020). What is IoT? The Internet of Things Explained: The Internet of Things (IoT) is a Network of Connected Smart Devices Providing Rich Data, but it can also be a security nightmare. *Network World (Online)*, Retrieved from https://www.proquest.com/trade-journals/what-is-iot-internet-things-explained/docview/2402564425/se-2?accountid=8289

Heuer, R. J., Jr, & Pherson, R. H. (2010). *Structured Analytic Techniques for Intelligence Analysis* (1st ed.). CQ Press.
Hughes, M., & Hayhoe, G. (2007). *A Research Primer for Technical Communication: Methods, Exemplars, and Analyses* (1st ed.). Routledge.
Jindal, F., Jamar, R., & Churi, P. (2018). Future and challenges of internet of things. Int. J. Comput. Sci. Inf. Technol, 10(2), 13-25.
Kaloudi, N., & Li, J. (2022). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
Kirtley, J., & Memmel, S. (2018). Too Smart for Its Own Good: Addressing the Privacy and Security Challenges of the Internet of Things. Journal of Internet Law, 22(4), 1–33.
Kumar, R. (2014). *Research Methodology: A Step-by-step Guide for Beginners* (4th ed.). Sage. Print.
Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A security framework for the internet of things in the future internet architecture. Future Internet, 9(3), 27.
Lockwood, J. (1993) "The Lockwood Analytical Method for Prediction (LAMP)." Joint Military Intelligence College. Print.
Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.
Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. In From active data management to event-based systems and more (pp. 242-259). Springer, Berlin, Heidelberg.
Nurse, J. R. C., Creese, S., & De Roure, D. (2018). Security Risk Assessment in Internet of Things Systems. https://doi.org/10.1109/MITP.2017.3680959
Paganini, P. (2021). *Your new smart car is an IoT device that can be hacked*. CyberNews. https://cybernews.com/security/your-new-smart-car-is-an-iot-device-that-can-be-hacked/
Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing, 6(5).
Rizvi, S., Kurtz, A., J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 163-168, doi: 10.1109/TrustCom/BigDataSE.2018.00034.
Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.
Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80, 1-50.
Rugge, F. (2018). *Confronting an "Axis of Cyber"?* Ledizioni. http://library.oapen.org/handle/20.500.12657/23931
Shpachuk, Y. (2022). *Healthcare IoT Security: Risks, Issues, Best Practices, and Our Advice*. Empeek. Retrieved October 18, 2022, from https://empeek.com/healthcare-iot-security-risks-issues-best-practices-and-our-advice/
Shuo-Yan Chou. (2019). The Fourth Industrial Revolution: Digital Fusion with Internet of Things. Journal of International Affairs, 72(1), 107–120.
Silex malware: Deadly new virus bricks 1000s of IOT devices. ALLOT. (2022). Retrieved January 17, 2023, from https://www.allot.com/blog/silex-malware/#:~:text=Your%20IoT%27s%20not%20sick%20%E2%80%93%20Someone,to%20all%20kinds%20of%20attacks.
Simon IoT. (2022). *The Rise of IoT: The History of the Internet of Things*. SIMONIoT.Com. https://www.simoniot.com/history-of-iot/
Statista. (2021). *Connected devices worldwide by access technology 2016–2021*. https://www.statista.com/statistics/774002/worldwide-connected-devices-by-access-technology/#:%7E:text=The%20statistic%20shows%20the%20number,devices%20amounted%20to%202.33%20billion.

Traynor, I. (2017, November 26). *Russia Accused of Unleashing Cyberwar to Disable Estonia*. The Guardian. https://www.theguardian.com/world/2007/may/17/topstories3.russia

U.S. Congress. (2016) 114th Congress. *Understanding The Role of Connected Devices In Recent Cyberattacks*. Www.Govinfo.Gov. https://www.govinfo.gov/content/pkg/CHRG-114hhrg23438/html/CHRG-114hhrg23438.htm

U.S. Congress. (2020). *H.R.1668 - 116th Congress (2019–2020): IoT Cybersecurity Improvement Act of 2020*. Congress.Gov | Library of Congress. https://www.congress.gov/bill/116th-congress/house-bill/1668#:%7E:text=This%20bill%20requires%20the%20National,physical%20devices%20and%20everyday%20objects.

Wei, W. (2018). *Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer*. The Hacker News. https://thehackernews.com/2018/04/iot-hacking-thermometer.html

Zhang, G. Q., Yang, Q. F., Cheng, S. Q., & Zhou, T. (2008). Evolution of the Internet and its cores. *New Journal of Physics*, *10*(12), 123027. https://doi.org/10.1088/1367-2630/10/12/123027