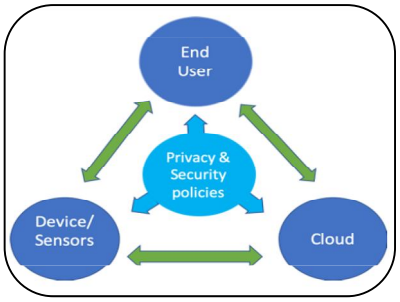
REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 9 | ISSUE - 6 | MARCH - 2020

IMPLEMENTATION OF SECURITY AND PRIVACY BY INTERNET OF THINGS

Joshi R. G.[1] and M. D. Acharya[2]
[1] Assistant Professor , Department of Computer Science, Yogeshwari Mahavidyalaya, Ambajogai.
[2] Assistant Professor , Department of Computer Science, Yogeshwari Mahavidyalaya, Ambajogai.

ABSTRACT:

The Internet of Things (IoT) is a technology that has the potential to revolutionize your lifestyle, from transportation to health, from entertainment to communication with government. This amazing opportunity also presents a number of significant challenges. The number of tools and the pace of their growth meet the challenges facing our security and freedom as we begin the battle to develop policies, standards and governance that shape this development without innovating. This paper discusses the evolution of IoT, its various definitions and some of its key areas. Security and privacy considerations and further challenges are discussed in general and in the context of these applications.



KEYWORDS: *Internet of Things (IoT) , transportation to health , further challenges.*

INTRODUCTION:

New technology has given users the ability to check their home security status from a smartphone, launch their car with a mobile phone app, and remotely open and close their garage door from anywhere in the world. These technologies are becoming part of what is known as the Internet of Things (IoT). In its most basic sense, IoT refers to the connection of everyday objects with the Internet. It monitors real time and collects huge amounts of information about assets, people, plants and animals. The Internet of Things (IoT) is a development that can dramatically change our lives. It is recognized as an enabler that increases efficiency in many sectors, including transportation and logistics, health and manufacturing. IoT will aid in process optimization through advanced data tics analysis and will be a catalyst for new markets leveraging its cyber physical characteristics along with the emergence of cross-cutting applications and services.

EVALUATION OF IOT:

A child grows every day and surprises their parents every moment, but still there are moments that mark milestones in their life history. Let us try to chronicle such milestone moments in the evolution of IoT:

- The ARPANET was the first connected network – the grandfather of the Internet as we know it. The history of IoT begins with ARPANET.

- In 1982, David Nichols, a graduate student in Carnegie Mellon University's computer science department, wanted to know if the department's Coke vending machines had bottles of cold soda. He was tired of going to the machine to find that no cold bottles were available; The vending machine was a few blocks away from his classroom. So he wanted to know in advance.
- He was assisted in this endeavor by Mike Cazar and Ivor Durham, two fellow students, and John Czarne, a research engineer at the university. The code they wrote can check whether a vending machine has Coke available, and if so, whether it's cold. Anyone on the ARPANET university can monitor the status of a Coke vending machine.
- In 1989, Tim Berners-Lee proposed the framework of the World Wide Web, which laid the foundation for the Internet.
- In 1990, John Romkey developed a toaster that could be turned on and off over the Internet. It was a wired toaster to the computer as there was no Wi-Fi back then!! This toaster is considered the first IoT device – the first "thing" to usher in the Internet of Things.
- Researchers and scientists seem to have a thing for caffeine - cold or hot. In 1993, the Trojan Room Coffee Pot was created by Quentin Stafford-Fraser and Paul Jardetsky in 1993 at the Cambridge University Computer Laboratory. An image of the interior of the pot was uploaded to the building server three times every minute. Later, when the browser starts displaying the images, these images can be viewed online.
- The next milestone in the development of IoT came in 1999 when Kevin Ashton, the current executive director of Auto-ID Labs, coined the term Internet of Things. A presentation he made to Procter & Gamble (where he worked at the time) was titled Connecting RFID in P&G's Supply Chain to the Internet.
- The term IoT began to be used in mainstream publications such as The Guardian and Scientific American by 2003-2004. During the same period the US Department of Defense and Walmart deployed RFID in their stores.
- The United Nations International Telecommunications Union acknowledged the impact of IoT in their report in 2005. IoT is predicted to help create an entirely new dynamic network.
- In March 2008, the first IoT conference was held in Zurich. It brought together researchers and practitioners from both academia and industry to facilitate knowledge sharing. In the same year, the US National Intelligence Council included the Internet of Things as one of six disruptive civilian technologies.
- In a 2011 white paper, the Cisco Internet Business Solutions Group (CIBSG) stated that the Internet of Things was born between 2008 and 2009 when the number of things connected to the Internet exceeded the number of people connected to it. CIBSG calculated that the ratio of people to things increased from approximately 0.8 in 2003 to 1.84 in 2010.
- Along with the white paper, Cisco published several educational materials on the topic and launched marketing initiatives to attract customers looking to adopt IoT. IBM and Ericsson soon joined the race.
- In 2011 Gartner included IoT in its hype cycle for emerging technologies.
- In 2013 IDC released a report that predicted the IoT market to grow at a CAGR of 7.9% and reach USD 8.9 trillion by 2020.

Related Risk with IoT:

IoT creates a massive attack surface by creating more access points on the Internet that need to be safely monitored. The higher the attack surface, the more vulnerability that can be used, therefore, bringing new equipment online into the home, office or other areas poses many new risks. In 2016 new, Europol identified these new threats: 'With more and more goods connected to the Internet and the creation of new types of critical infrastructure, we can expect to see targeted attacks on existing and emerging infrastructure, including new types of blackmailing and ransom schemes. Data theft, physical injury and potential death and new types of botnets.

- **Lack of physical rigidity:** Lack of physical rigidity has always been a concern for devices in the Internet of Things. Since most IoT devices are deployed remotely, there is no way to properly secure devices that are in constant contact with a widespread physical attack surface. Unsecured devices and the inability to maintain constant surveillance allow potential attackers to gain valuable information about their network capabilities that could aid in future remote attacks or device control. For example, hackers can read the contents of a memory card to remove it and access private data and information that can give them access to other systems.
- **Insecure data storage and transfer:** As more people use cloud-based communications and data storage, cross-communication between smart devices and IoT networks increases. However, when data is transferred, received or stored over these networks, the possibility of a breach or compromise also increases. This is due to the lack of encryption and access controls before entering data into the IoT ecosystem. For this reason, it is important to ensure the secure transfer and storage of data through robust network security management tools such as firewalls and network access controls.
- **Lack of visibility and device management:** Many IoT devices remain unmonitored, untracked and improperly managed. As devices connect and disconnect from the IoT network, trying to monitor them can become very difficult. Lack of visibility into device status can prevent organizations from detecting or responding to potential threats. When we look at the healthcare sector, these risks can be life-threatening. IoT pacemakers and defibrillators have the potential to be tampered with if not properly secured, and hackers can intentionally destroy batteries or deliver incorrect pacing and shocks. Organizations need to implement a device management system to properly monitor IoT devices so that all avenues for potential breaches are considered.
- **Botnets:** Botnets are a series of Internet-connected devices designed to steal data, compromise networks, or send spam. Botnets consist of malware that allows an attacker to access an IoT device and its connections and infiltrate an organization's network, becoming one of the biggest threats to businesses. They are most prominent in devices that were not designed to be safe to begin with (for example, smart fridges). These devices are constantly morphing and adapting. Therefore, it is necessary to monitor their changes and threat patterns to prevent attacks.
- **Weak passcodes:** Although complex passcodes prove to be secure for most IoT devices, it only takes one weak passcode to open the gateway to your organization's network. Inconsistent management of passcodes across the workplace enables hackers to compromise your entire business network. If even one employee does not follow advanced password management policies, the likelihood of a password-driven attack increases. Practicing good password hygiene is essential to ensure your business covers all bases under standard security practices.
- **Insecure ecosystem interfaces:** Application programming interfaces (APIs) are software intermediaries that allow two applications to talk to each other. With the connection of two servers, APIs can present a new gateway for attackers to access business IoT devices and breach the network's routers, web interfaces, servers, etc. It is important to understand the intricacies and security policies of each device ecosystem before connecting them to ensure overall network security.
- **AI-Based Attacks:** While AI attacks have been around since 2007, the threats they pose in IoT are becoming more prominent. Hackers can now create AI-powered tools that are faster, easier to scale and more efficient than humans to carry out their attacks. This poses a serious threat to the IoT ecosystem. While the tactics and elements of traditional IoT threats presented by cyber attackers may seem similar, the scale, automation and customization of AI-powered attacks will make them more difficult to combat.

Securities of IoT:

If security issues are widespread among IoT devices known to be vulnerable, class actions and product liability lawsuits may be filed against IoT device manufacturers by affected consumers. Other

IoT stakeholders may also be held accountable; This will be determined by their level of responsibility for the event that caused the damage or caused the damage. In addition, companies in the USA may be charged under the Federal Trade Commission Act of 1919 for unfair or deceptive practices that adversely affect the safety and privacy of consumers. U.S. According to the Federal Trade Commission, TREND Net's 'practice may cause or cause substantial harm. Customers or customers who are not in the best interest of competition and customers cannot be avoided. In its enforcement action, the U.S. The Federal Trade Commission accused TRND Net of undermining security practices and misleading consumers by claiming their IoT devices were secure. In fact, these devices contained flawed software, exposing the private lives of hundreds of consumers; In particular, the hacker exploited a software flaw and posted links to live feeds of nearly 700 consumer cameras. Protecting IoT devices and detecting threats requires the use of proactive firewalls and comprehensive security systems. An example of such software is BitDefender. BitDefender is currently promoting one of its products, the BitDefender Box, to protect everyday objects connected to a home network from malicious software. Additionally, to protect IoT devices, common security practices and standards are required. However, not every IoT device requires the same level of security. 'Devices that collect sensitive information, devices that pose a physical security or safety risk, or communicate with other devices or networks in a way that would allow intruders to access those devices or networks rather than room temperature control devices, including miles or calories.

Management of Identity and Validation:

Authentication in IoT is critical, as privacy, integrity, and system availability can be compromised without proper authentication. This is because if an adversary is able to authenticate as a legitimate user, they will have access to any data the user has, and the user can view, modify, and delete or restrict its availability that way. Identifying and identifying users in IoT is a key challenge. Currently, username/password pairs are the most common form of authentication and user identification in electronic systems, although shared keys can be used in other ways, such as digital certificates or biometric credentials. However, portraying the IoT as ubiquitous will eliminate most of the physical interactions that provide usernames and passwords. The ability to leverage single-sign-on (SSO) systems can be useful in traditional electronic environments, allowing users to authenticate only once to interact with different services. Systems like Shibboleth Open ID and Ooth are not designed to complement IoT systems, and although work is being done to optimize Ooth, it cannot provide comprehensive SSO in an IoT environment. Citizens in an IoT environment can choose their identity provider and using existing protocols is challenging.

Privacy Challenges in IoT:

Privacy is seen as a major concern in IoT, and IoT has provided a wealth of data not only to the World Wide Web, but also to ordinary citizens, groups, and organizations. It can be used to establish what interests you, where you go, and your purpose. This may lead to better opportunities for improved services, but it must be weighed against our desire for privacy. It is crucial that consumers trust the services they invest in to respect their privacy. Trust is a fundamental factor in building any relationship and is an important factor in adopting new technologies. People will not use new technologies unless they have sufficient confidence in the protection of privacy, security and safety, and this is true in complex systems such as IoT. On purpose, there are billions of IoT devices; Each of them is designed to collect, store and communicate data. This data can be easily used for real-time information about a person's health and finances, locations, contacts, habits, behavior and activities. Apart from disclosing this type of personal information, this data can also be used to detect changes in the routine and unusual behavior of individuals. Ultimately, IoT devices create an environment where information about each individual can be stored, analyzed, monitored, made available, and shared with other networking devices and potentially other users. As IoT devices, people and companies collect, process, store and exchange information about individuals, there is a significant opportunity to create a detailed account of the private lives of millions of users. Privacy is an essential human right and is protected in

domestic, regional and international human rights instruments. An essential element of privacy is the ability to keep something secret. IoT users may find it difficult to 'keep things secret' because 'the full development of IoT capabilities may strain the current possibilities of anonymous services and generally limit the possibility of being unnoticed'. Another essential element of privacy is the right to control and access others' information about oneself. Users may find it difficult to control their information as communications and data exchanges between IoT devices can be 'triggered automatically' as well as by default, without anyone noticing'. In order to protect personal data, self-regulation by consumers is advocated. Individuals should be able to control and choose what data is collected, who stores it and when. IoT is basically a repository for every aspect of a person's life. At a minimum, 'applications should facilitate the exercise of the right to access, modify and delete personal information collected by IoT devices'. Additionally, users must consent to the use of an IoT device and the data collected by the device is 'information' and free. Users should not be penalized or denied access to their device's capabilities if they decide not to use the device or certain services. 'Currently, users can be fined or denied access to important services for choosing not to 'opt-in' or 'consent' to the collection of their data. U.S. In the automotive industry, 'customers who do not consent to data collection may be denied access to valuable vehicle features. For example, the only way consumers can turn on navigation features in their vehicles is to share geolocation information for marketing purposes.

CONCLUSION:

Securing IoT devices is a multifaceted and complex process. An inadequate legal framework requires immediate action in legal analysis of existing risks and may require a new approach in law. To effectively address existing IoT vulnerabilities, it is recommended that existing applicable legal frameworks be thoroughly analysed and, if necessary, new elements be developed to address the risks associated with IoT deployments.

REFERENCES:

1. Beatty, Patricia, Ian Reay, Scott Dick, and James Miller (2007), “P3P Adoption on e- Commerce Web Sites: A Survey and Analysis.” IEEE Internet Computing 11 (2): 65–71.
2. Carsten Maple (2017), “Security and privacy in the internet of things”, Journal of Cyber Policy, 2:2, 155-184.
3. Lo’ai Tawalbeh, Fadi Muheidat , Mais Tawalbeh and Muhannad Quwaider, 2020. IoT Privacy and Security: Challenges and Solutions. Applied Science, MDPI. 10(4102): 1-17.
4. Mardiana binti Mohamad Noor, Wan Haslina Hassan, 2020. Current research on Internet of Things (IoT) security: A survey. Computer Network, 148(2019):283-294.
5. Shantanu Pal, Michael Hitchens, Tahiry Rabehaja and Subhas Mukhopadhyay, 2020. Security Requirements for the Internet of Things: A Systematic Approach. Sensors, 20, 1-35.