International Journal of Hyperconnectivity and the Internet of Things
Volume 7 • Issue 1

A Strategic Approach to IoT Security by Working Towards a Secure IoT Future

M'Kaila J. Clark, SUNY Empire State College, USA
Lila Rajabion, SUNY Empire State College, USA*

ABSTRACT

The internet of things' (IoT) fast-growing development and adoption are undeniable. Although the IoT development is moving at a fast rate, the security of these technologies is not keeping up. Lack of security infrastructure on the internet of things is due to such security measures being excluded from the average company business plan and the lack of security configurations established. The increasing need for robust security architecture is needed to address said vulnerabilities. How do the internet of things companies create a dynamic security approach to defend and combat threats while also being flexible to accommodate future technological advancements? This paper will answer this question by addressing the strategic approach to developing a strong IoT security infrastructure that promotes confidentiality, integrity, and availability with dynamic elements that allow for future developments to address new security concerns. This research question will be answered through analysis of extensive thematic literature review.

KEYWORDS

Availability, Confidentiality, Cybersecurity, Integrity, IoT, Security Infrastructure

INTRODUCTION

IoT devices are used to record and transfer data to monitor important processes, give new insights, increase efficiency, and allow for companies to make more informed decisions. The IoT market that includes hardware, software, systems integration, and data telecom services has projected to grow to $520 billion by the end of this year. This figure represents more than a 100 percent rise from 2017s $213 billion spent. In a matter of a few years, significant growth in the IoT market has been displayed, thus indicating that many organizations are taking advantage of its benefits at a fast rate. Many organizations have IoT to thank for their organizational advancements and this growing adoption is actively encourage other organizations to adopt an IoT infrastructure in hopes to reap the same benefits.

While businesses are quick to apply IoT devices to enhance their business, many industries are not prepared to protect these devices. Many industries lack a security and privacy program, lack ownership and governance to drive privacy and security, lack the incorporation of security into the design of products and ecosystems, have insufficient security and awareness training for engineers and architects, lack security resources, have insufficient monitoring devices and systems to detect

DOI: 10.4018/IJHIoT.317088 *Corresponding Author

threats, lack of post-implementation risk management, lack of visibility, still follow legacy security practices, and have inexperienced incident response processes. Many businesses fail to see the urgency in apply comprehensive security measures and instead are hyper-focused on the beneficial aspects it provides to their business. Many organizations are unaware of how to prevent and protect their newly incorporated devices, and many neglects to consider the security risks entirely.

BACKGROUND

Current State of IoT

The internet of things (IoT) is an industry on the rise and is projected to continue its rapid growth in the years to come. IoT is one of the various underlying drivers behind the internet evolution. IoT is the internet factor improving the business world by increasing processing power, storage capacity, network capability, and dramatically lowered costs through microchips, sensors cameras and accelerometer implementation into the everyday device. These are some of the benefits that drive the adoption of IoT in the business setting. Many industries are taking advantage of the benefits of IoT. These industries include manufacturing, aviation, the supply chain, agriculture, and healthcare. Many other industries are also creating more data streams and analytics potential, which means companies gain much greater insight into their business operations and how their customers use and respond to their products and services.

IoT is slashing both operational costs and downtime in factories and industries and assisting with worker learning on the job via tablets, AR Headsets, and smart goggles. IoT enables businesses to connect key business processes, which can, in turn, allow leaders to identify ways to boost efficiency and productivity more easily. Asset tracking and waste reduction are also benefitting of IoT tracking mechanism adopted by industries. IoT also gives birth to new business models derived from tracking data gathered through IoT devices. These are some of the many benefits to businesses and display IoT technology expansion that creates for more digital transformation. Recent projections anticipate that IoT technologies will have a massive impact in societies technological and economic impact thus, driving many businesses to adopt IoT with the intent of preserving business longevity and being able to meet new business demands that arise because of IoT. Trillion in value is projected to be crated through cost-savings through preventive health care, minimized accidents, patient monitoring, efficiencies in manufacturing and distribution industries.

Security Threats Associated With IoT Adoption

The adoption of the internet of things has led to the incorporation of interconnected devices amongst organizations however it has also served as an interconnection of threats. Threats associated with IoT include phase attacks, data reach, data sovereignty, data loss, data authentication, attacks on availability, flooding by attackers, flooding by legitimates, external attacks, modifications of sensitive data, distributed denial of service attacks Botnets, Byzanite failure, and more. The attacks that are most prevalent in the adoption of an IoT infrastructure include DoS attacks, spoofing, malware, eavesdropping, network layer attacks, and breaches.

Each threat poses a unique set of damages to an ill secured IoT infrastructure. Denial of service attacks or DoS can cause damages to an organization's finances, reputation, and greatly hinders the organizations data availability. The financial damages of DoS depend on the size of the organization and finances at stake but can lead to the loss of millions of dollars based on the organization attacked. In addition to the financial losses that occur as a result of DoS this attack can greatly affect an organization reputation, possibly marking it as one that is poorly secured. A poor reputation brought on by a DoS attack can lead to the ceasing of current business partnerships and prevent the development of future partnerships. DoS greatly affects the availability of data resulting in data that is inaccessible to authorized users that will impede upon organizational operation.