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.

Spoofing can cause intrusive damages allowing external attackers access to your system. Attackers spoof RFID signals to record data transmissions from an RFID tag. Attackers can use this spoofed RFID tag to then send their own data containing original tag ID which will inevitably allow intruders full access to your system to do with your data as they choose and inevitably leading to breaches of information. Further intrusive attacks like eavesdropping can lead to confidentiality breaches and financial loss. Eavesdropping attacks open the door for attacks such as ransomware which can lead to attackers blocking off access to data only to open it in exchange for finances. Whether or not an organization provides said funds it is likely that they will suffer tremendous financial loss. Eaves dropping attacks also allow for attackers to gain access to confidential and may even lead to stolen credentials by listening into private conversations.

Malware attacks can result in an organization infected device being turned into bots, rendering these devices completely inoperable. Malware injections have the potential to permanently deny service. Network layer attacks can result in the compromission of the IoT architecture at the perception layer, network layer, middleware-layer and application layer thus serving to be a compressive and layered attack if all layers are targeted. Security breach result in damages to reputation and loss of finances and partnerships. The breach of security also violates confidentiality and will result in a poor reputation organization being identified by their lack of secure system infrastructure and breach of confidential data.

Assessing Organizational Susceptibility for IoT Threats

As organizations adopt IoT they neglect the adoption of a solid IoT security infrastructure and see IoT security as an afterthought leaving them riddled with vulnerabilities. The lack of IoT security incorporated means that there a lack of consistent security mechanisms in place to ensure password security, encryption and granular user access permissions. The current vulnerabilities that many organizations face include privacy concerns, insufficient authorization, lack of transport encryption, insecure web interfaces and inadequate software protection.

As IoT continues to rise the diversity in connected devices will rise as well and with-it increased security concerns and vulnerabilities. Spikes in the demand for IoT production will push manufactures to quickly bring to the market new connected devices, cloud accessibility, and mobile applications to gain share. The demand of new IoT devices and capabilities results in new unsecured technologies. As quantity and new development takes priority with the rising demand for new IoT security becomes left out of the manufacture's development processes. The lack of focus on the entire IoT infrastructure and lack of comprehensive approaches applied to new IoT results in new devices that lack basic device security mechanisms. Thus, neither manufacturers or organization consumers have security as a focal point or even at the very least a consideration.

Many organizations lack the extensive planning necessary prior to IoT implementation. IoT implementation planning is a crucial part of the entire implementation process and it is important that everything is considered during the planning phase. However, many organizations fall short in the planning phase and fail to consider the crucial IoT security concerns which include an insecure web interface, privacy issues, improper authorization mechanisms, cloud interface insecurity, insecurity in mobile interfaces, insecurity in network interfaces lack of physical security, software security, configuration issues and the lack of transport encryption. These areas are all critical elements of the planning to consider, as without consideration of these areas can cost an organization its future.

Failure to forecast data volume can be a major mistake in IoT implementation of devices and applications as well which can result in the swelling of both structure and unstructured data. The swelling of this data is due to the lack of an organizations ability to forecast data volume resulting in the businesses not choosing the appropriate IoT big data businesses strategies necessary to properly manage large amounts of data. Lack of proper plans for device updates and replacements are also an ongoing organization IoT implementation shortcoming. Lacking mechanisms for updates and

replacements threatens device reliability and data availability. Realistic IoT implementation timelines also pose an issue resulting I businesses rushing implementation and leaving out security controls.

Plan to Defend Against Threats

Strategic plan development is a must when planning a design of a secure IoT infrastructure. To form a strategic plan all security concerns must be considered so that the proper security control can be planned for. To defend against threats, all threats especially those that are most prevalent in IoT must be identified and the weight of the threat measure. The weight of the threat will be measured by the level of damages it has the potential to cause the organization. Knowing of all potential threats, most prevalent threats and of projected damage if affected by such threats allows organizations to plan specifically based upon the challenges, they could face the amount of damage exploitation of certain vulnerabilities could cause. Thus, the strategic plan development should consider all threats, frequent threats, and the weight of these threats.

Making the Security Plan Comprehensive

To develop a comprehensive security plan all common threats should be first classified so that the appropriate countermeasure is applied. Counter measure will depend upon the type of threat classification. The classifications are based on the specific type of common threat. The most common threat classifications of IoT include DoS attacks, spoofing, various intrusive attacks, malware, eaves dropping, network layer specific threats, and security breaches. All of these threat classifications are detailed in Table 1: IoT Threat Classifications and Counteracting Security Mechanisms. These threat classifications and counteracting security mechanisms have been derived from collective research on other IoT security journals all of which recorded the same IoT threat tendencies with various unique approaches. These approaches and threats are consolidated in Table: 1 IoT Threat Classifications and Counteracting Security along with references to the threat and counteractive measure origin (see Table 1).

Table 1 IoT Threat Classifications and Counteracting Security Mechanisms also details the corresponding threats counteractions. The security attacks listed in Table 1 include Dos attacks, Spoofing, intrusion, malware, eavesdropping, and threats tailored specifically to IoT architecture layers and security breaches. Some of the key results of this table are the various machine learning security methods and the positive security outlook this comprehensive approach is projected to have. The different machine learning-driven methods used to combat threats such as DoS attacks, Spoofing, intrusion, malware, and eavesdropping include neural network, multivariate correlation analysis, Q-learning, SVM, and K-NN. The neural network is a detection engine used to flag known and unknown attacks from traffic. Multivariate correlation analysis enables the distinguishability of normal traffic and attack traffic. This analysis involves the investigation and extraction of second-order statistics from observed network traffic. Q-learning is an effective machine learning technique to authenticate normal traffic from attacker traffic. SVM or support vector machines successfully detect intrusion via pattern recognition. K-NN of the K-nearest neighbor classifier successfully uses algorithms to identify abnormal nodes via comparing the distance function and cutoff value of each node. All of these methods have their own projected outcome based on threat, but they all share the outcome of creating a secure IoT infrastructure that maintains the core elements of confidentiality, availability, integrity, and privacy.

MAKING THE SECURITY PLAN STRONG

A strong and well developed IoT security infrastructure plan will require the investment of many organization members especially those in executive level management all other stakeholders that can

Table 1. IoT Threat Classifications and Counteracting Security Mechanisms

IoT Security Threat	Threat-based Security Method(s)	Method Rationale	Projected Outcome	Article Referenced
DoS attacks	Neural network Multivariate correlation analysis	-The neural network is a detection engine used to flag known and unknown attacks from traffic. -Multivariate correlation analysis enables the distinguishability of normal traffic and attack traffic. This analysis involves the investigation and extraction of second order statistics from observed network traffic. Effective machine learning technique to authenticate normal traffic from attacker traffic.	-IoT infrastructure has a secure IoT offloading and strong access controls preventing DoS attacks.	Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use ai to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41-49. doi:10.1109/msp.2018.2825478 (Continued)
Spoofing	Q-Learning -Distributed Frank Wolfe and incremental aggregated gradient	**-** Effective machine learning technique to authenticate normal traffic from attacker traffic. **-**The techniques Frank Wolfe and incremental aggregated gradient can be applied to improve spoofing resistance.	**-**IoT security infrastructure is equipped with strong authentication methods to prevent spoofing.	Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use ai to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41-49. doi:10.1109/msp.2018.2825478
Intrusion	SVM Habitual hardware and software security implementations K-NN Neural network Tickets IoT-Zone Identification IoT Token Generation	-Support vector machines successfully detect intrusion via pattern recognition. -Timely OTA updates and secure session key generation will aid in preventing exploitable points of entry and ensures authorization to appropriate users. The K-nearest neighbor classifier successfully uses algorithms to identify abnormal nodes via comparison of the distance function and cutoff value of each node. - The neural network detection engine detects possible intruders. -The use of tickets and sessions provides a secure access control method. This method utilizes tickets that are unique, unforgettable and cryptographically protected data sets these tickets are used to establish and confirm a session. - This allows for the active monitoring of user IoT trails as they navigate through various the IoT Zone that are marked by rule-based connectivity preventing unauthorized access and intrusions. -This token will serve as an authentication token for users. Users receive this IoT token through enrollment with the enrollment certificate authority, this certificate and the users public key are then used to gather transactions and from blockchain establishing the users trail and enabling the IoT activity to be monitored an intruder without valid authenticators identified. -IoT-hubs query tokens from a collection of nearby user devices via API and then verifies this by utilizing the blockchain network.	-IoT infrastructure has various access controls in place to prevent unauthorized access and intrusion.	Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer iot: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine, 9*(2), 17-25. (Continued) doi:10.1109/mce.2019.2953740 Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use ai to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41-49. doi:10.1109/msp.2018.2825478 (Continued)
Malware	Software integrity checks Secure software APIs	-The chain of trust will involve the secure and verified booting process. The chain of trust incorporates a key system used to verify trusted parties and ensure the validity of firmware and confirm it has not been injected with malware. -Data checks on the back end as well as authorization and authentication focus on the front end can make for a more secure API.	**-**Strong access controls and malware detection mechanisms are in place to prevent malicious code injection.	Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer iot: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine, 9*(2), 17-25. doi:10.1109/mce.2019.2953740 (Continued)

continued on following page

Table 1. Continued

IoT Security Threat	Threat-based Security Method(s)	Method Rationale	Projected Outcome	Article Referenced
Eavesdropping	VLFSR lightweight encryption function Random key agreement Q-Learning Non-parametric Bayesian	-The VLFSR encryption function is successful against large scale RFID attacks. This encryption function can also be utilized in the design of RFID security protocol with efficient hardware requirement to meet the secure and low-cost RFID system demands. -The random key agreement is a practical and energy efficient key to secure duplex near-field communication -Effective machine learning authentication -method. -The non-parametric Bayesian method aids in the evaluation of the RSSI and the packet arrival tie intervals of the ambient radio signals to detect potential eavesdroppers and spoofers that are out of proximity.	-Authentication mechanisms are implemented In the IoT infrastructure creating for a safe IoT environment safe from large scale RFID attacks.	Ivan, C., Vujic, M., & Husnjak, S. (2016). Classification of security risks in the IoT environment. *DAAAM Proceedings,* 0731-0740. doi:10.2507/26th.daaam.proceedings.102 Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use ai to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41-49. doi:10.1109/msp.2018.2825478 (Continued)
Threats to the layered IoT architecture (perception layer, network layer, middle-ware layer, and application layer.	Secure communication	-Secure communication can be incorporated to using authentication, security policies, key management between devices, gateways, M2M components, service layer M2M security, and transparent middleware using authentication via encryption mechanisms.	-All IoT architecture layers are secure and authentication methods work effectively.	Ivan, C., Vujic, M., & Husnjak, S. (2016). Classification of security risks in the IoT environment. *DAAAM Proceedings,* 0731-0740. doi:10.2507/26th.daaam.proceedings.102 (Continued)
Security breaches/ leaks of information	Hardware Obfuscation	-Hardware obfuscation protects devices intellectual property by securing information on-chip information to prevent reverse engineering attacks.	-Data housed within the IoT infrastructure is secure and confidentiality is maintained.	Ivan, C., Vujic, M., & Husnjak, S. (2016). Classification of security risks in the IoT environment. *DAAAM Proceedings,* 0731-0740. doi:10.2507/26th.daaam.proceedings.102

support a strong IoT security initiative both financially, legally and on a corporation level. Identifying and balancing the needs of stakeholders is a challenging part of making the security plan strong however, the benefits of the support provided by stake holders supersedes the effect of the challenges that come with the pressure off appealing to so many stakeholders. Key stakeholders that will provide valuable contribution and support include executives, finance, operations, engineering, IT, legal and data science. Once support is gain by all or most of these stakeholders then the plan now how the approval and endorsement needed to progress and move to the next phase in the security plan process.

The threat response team is also an integral factor in the planning phase. The threat response team is going to lead efforts of the plan design based on the classifications of threats. The threat teams contributions are crucial as they will ensure that the security plan is closely aligned with threat classifications, thus increasing the probability that all the proper security controls are incorporated. The threat response team will also ensure that each threat solution is closely evaluated prior to implementation.

A clearly outlined plan results in the development of a fully outlined strategic plan. The strategic approach that will prove to because a comprehensive security system is what I refer to as the Atmospheric IoT Security approach. The Atmospheric IoT security approach is an analogy for the layered security approach that is necessary in securing an IoT environment. At the very core of each security layer is IoT similar to that of the Earth that is at the center of various atmospheric layers ranging from troposphere to exosphere. Each atmospheric layer serving its interictal purpose in the Earth's stability as the layers pf security mechanism that ensure IoT stability.

The atmospheric IoT security approach is centered around protection needed for the most prevalent IoT threats. The Atmospheric IoT Security approach is comprised of security mechanisms that counteract the common IoT threats include DoS attacks, spoofing, intrusion, malware, eavesdropping, advanced persistent threats, man-in-the-middle attacks, remote recording, ransomware, Botnets, and

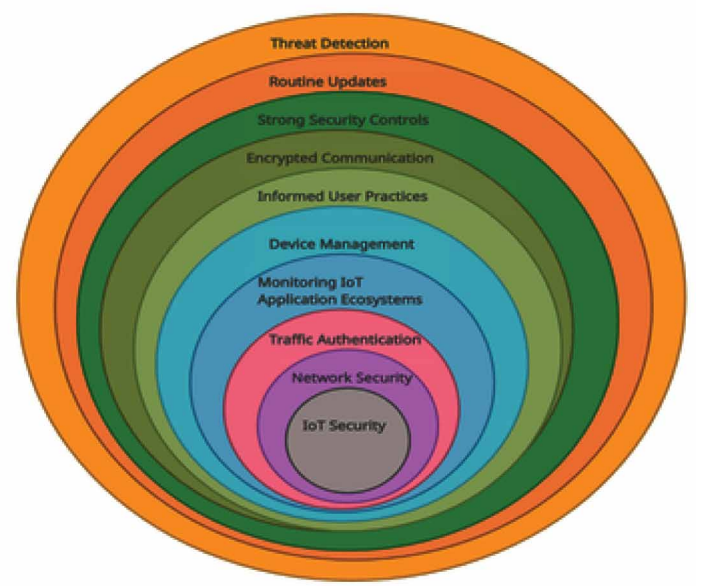
social engineering attacks. Each potential attack prompts a specified layer of protection to add to the IoT infrastructure. These atmospheric security layers include network security, traffic authentication, threat detection, routine updates, robust security controls, encrypted communication, informed user practices, device management, monitoring IoT application ecosystems, and hardware security. These security layers are illustrated in the Figure 1: Atmospheric IoT Security Infrastructure (see Figure 1).

MAKING THE SECURITY PLAN DYNAMIC

The atmospheric approach was an approach I was able to develop after an extensive thematic literature review. After my thematic literature review, I consolidated my results, and these consolidated results are what is depicted in Table 1: IoT Threat Classifications and Counteracting Security Mechanisms. After consolidating results, I was able to form each atmospheric layer according to its prominent threat. Included with my research apparatus is the Google scholar search engine as well as consumer survey results and industry studies from Statista a leading statistics portal. I also formulate my approach through a basic procedure in which I first analyze all IoT security vulnerabilities and tendencies gathered through literature review, reviewed current IoT security infrastructure shortcomings, listed some factors to include in dynamic approach development and analyzed the projected outcomes of strategic IoT security architecture implementation. This procedure and thought process is illustrated in Figure 2: Strategic IoT Security Approach Conceptual Framework (see Figure 2).

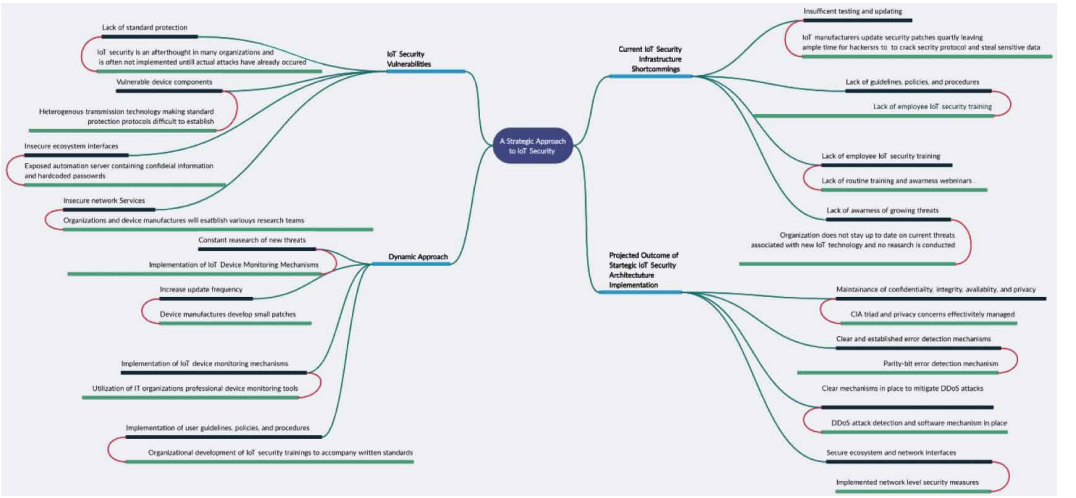
A crucial factor that can be attributed to the success of an IoT security plan is its dynamic nature. A robust IoT security plan will uphold the utmost level of security as it will address an array of threats and detail counteractive defense, risk detection, and mitigation mechanisms. For IoT security infrastructure to be dynamic it must not only be multilayered, but it must also be flexible. The multilayered approach will ensure the strength of the infrastructure as all major security threats and levels of threats will be met with its tailored defense layer. The flexibility of the approach will ensure the longevity of the approach and determine its relevance and ability to adapt to the changes

Figure 1. Atmospheric IoT Security Infrastructure



Note: The model above is the visual representation of the atmospheric IoT security infrastructure framework.

Figure 2. Strategic IoT Security Approach Conceptual Framework



in technology and meet new security threats. Lacking this dynamic security infrastructure can leave organizations ill equipped to handle future threats and can result I catastrophic damages.

To develop a strategic IoT security in infrastructure an organization can adopt the atmospheric approach or model a similar approach that is aligned in the same manner. The Atmospheric IoT Security approach is dynamic in nature and is comprised of nine layers formed on the premise of the most prominent threats that surround IoT. Each layer encompasses the core, that in figure 1 is illustrated as IoT security. The IoT security core serves as a root, signifying that each layer of protection is maintaining the core, keeping the overall security of the internet of things. Each layer can equate that of a shield providing for the ultimate multifaced and strategic approach. The network layer is equipped with various network security methods such as neural networks, multivariate correlation analysis, and secure communication practices. The traffic authentication layer includes mechanisms such as Q-learning, multivariate correlation analysis, and neural network. The monitoring IoT application ecosystems layer includes various application programming interfaces such as secure software API, and IoT token generation.

The device management layer consists of habitual hardware security implementations and hardware obfuscation. The informed user practices layer entails tracking and managing of devices, patching and remediation, and testing and evaluation. The encrypted communication layer includes VLFSR encryption and secure communication policies and procedures. The strong security control layer consists of software integrity checks, secure software APIs, and hardware obfuscation and distributed Frank Wolfe and incremental aggregated gradient. The routine updates layer includes habitual hardware and software security implementations. Lastly, the threat detection layer is comprised of neural network, multivariate correlation analysis, support vector machines and non-parametric Bayesian.

Neural networks are a strong detection engine that will flag unknown usage and attacks from traffic making it an integral security method at the network security layer. Also at the network security layer is multivariate correlation analysis that enables the distinguishability of normal traffic and attack traffic. Multivariate also involves the investigation and extraction of the second order statistics from the observed network traffic. Secure communication methods at the network security layer are incorporated using authentication security policies. At the traffic authentication layer Q-learning serves as an effective machine learning technique to authenticate normal traffic from attacker traffic. Multivariate correlation analysis also found at this layer and contributes investigative and extraction

methods based on aggregated statistics observed from network traffic. The neural network at the traffic authentication layer is an additional network detection engine that flags unknown attacks from traffic.

At the monitoring IoT application ecosystem layer secure software API checks data on the back end as well as authorization and authentication focus on the front end making for a more secure API. IoT token generation at this layer serves as an authenticating token for users. IoT token generation prompts the distribution of authentication tokens to users and the token is received through enrollment with a certificate of authority, the certificate and the users public key are then used to gather transactions from blockchain establishing the users' trail. While establishing the user's trail and enabling the IoT activity to be monitored an intruder without a valid authenticator can be appropriately identified. Habitual hardware and software security implementations at the device management layer involves timely updates and secure session key generation that aids in preventing exploitable entry points while also ensuring authorization to appropriate users. Also, found at the device management layer, hardware obfuscation protects devices intellectual property by securing information on-chip information preventing reverse engineering attacks.

At the informed user practices layer practices such as tracking and managing of devices, patching and remediation, and testing and evaluation are critical user capabilities that will ensure all devices properly manage and appropriate patches, tests, and evaluations are initiated to prevent exploitation risk. The encrypted communication layer is well equipped with the VLSFR encryption function that proves successful against large scall RFID attacks. The VLSFR encryption function can also be utilized in the design of RFID security protocol. Secure communication policies and procedures also located within this layer, are a strong method that enforces authentication and security policies and procedures. Software integrity checks at the strong security controls layer serves as a chain of trust that involves the secure and verified booting process. The chain of trust incorporates a key system that is used to verify the validity of trusted parties as well as the validity of firmware and confirm that no malware injections have taken place. Secure software APIs at this layer involve data checks used on the back end as well as authorization and authentication focus on the front end to ensure a secure API. Hardwar obfuscation that this level will secure intellectual property on-chip. The distributed Frank Wolfe and incremental aggregated gradient improves resistance to spoofing.

The habitual hardware and software security implementations found within the routine updates layer promote timely OTA updates and secure session key generation and assist in preventing points of entry to authorized users. The neural network and multivariate correlation analysis at the detection layer serve as detection methods to distinguish between trusted and untrusted traffic. Support vector machines at tis layer successfully detect intrusion via pattern recognition. The detection layer also includes the non-parametric Bayesian method that aids in the evaluation of the RSSI and the packet arrival tie interval of ambient radio signals to detect potential eavesdroppers and spoofers that are out of proximity.

THE FUTURE OF IOT AND THE EVOLVING SECURITY NEEDS

Soon a dramatic increase in IoT technology development and implementation can be anticipated. In the years to come development in IoT manufacturing, big data analytics, machine learning, healthcare adoption of IoT, smart city emergence and increased use of IoT to better workforce management. In the wake of the COVID-19 pandemic many businesses have found themselves technologically advanced beyond their expectations as many businesses have now incorporated and are continuing to incorporate IoT into their businesses. IoT has proven that not only is it here, but it is here to stay. Explosive growth if IoT uses and adoption promise great opportunities for businesses who join the IoT as well as ensure IoT longevity in the business sector.

Statistics project that IoT will shape the future and these projections are substantiated from collected statistics from various business sources. These sources include Cission, PR Newswire, Disruptive Asia, Microsoft, and Statistica. The adoption of smart devices to access the internet of things

increases yearly. In 2019 alone 26 billion IoT devices were active. According to the 2017 leadership project Disruptive Asia, businesses are already responsible for 57% of overall IoT spending. Smart cities have seen a recent incline as well in 2020 as many smart cities emerged that used IoT sensors to collect data and generate insight for better management. According to reports from Microsoft almost all business will be utilizing some form of IoT by the end of 2021. We can expect to see the IoT utilization in the core IoT industries such as manufacturing, retail, transportation, government, and healthcare, as these industries will continue to incorporate new IoT applications and solutions in their daily operations.

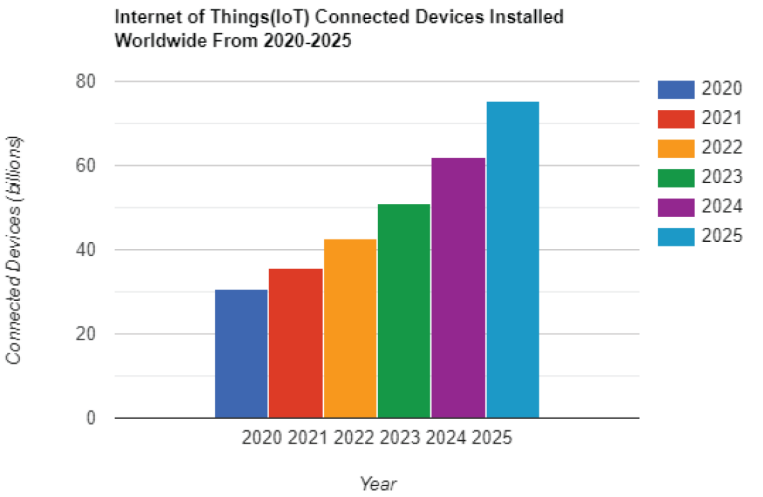
According to Statistista the projected global spending of IoT in the year 2023 is predicted to be at a value over 1.1 trillion dollars. This value is also projected to continue its steady growth throughout the years that follow. Statista also reports on IoT's demonstrated potential to save us money, with wireless cars generating over 5.6 trillion dollars in savings world-wide and IoT in agricultural technologies set to reduce food prices by nearly have by the year 2050. According to news distributions services like Cision PR Newswire the IoT market has an incredible compound annual growth rate of 24.7% and big names such as Google, Cisco, Microsoft, Apple, Dell, and Facebook amongst others are investing heavily in IoT applications. Figure 2: Projected IoT Trends displays the increase in billions of connected IoT de4vices over the course of 5 years.

In figure 3: Projected IoT Trends it is clear the direction at which IoT is taking over the course of the next 4 years. In the year 2020 there were approximately 30.73 billion connected devices world-wide. This 30.73 billion increased to 35.82 billion in 2021. It is predicted that by the year 2023 the number of connected devices will be 511.11 billion, this will increase to about 62.12 billion connected devices by the year 2024. Finally, by the year 2025 we can anticipate that approximately 75.44 billion connected devices will be in use worldwide.

With the explosive growth and adoption of IoT taking place and projected to take place I the near future businesses are presented with great opportunities for businesses to join the revolution of IoT and enhance their business operations. Such business operations that can be improved by the use of IoT include daily operations, asset tracking, waste reductions, streamline productivity, monitor all aspects of business, improve remote work capabilities, better data management solutions and more.

Despite the advantageous nature of organizational IoT adoption, these benefits are accompanied by a growing set of security concerns that only a multi-faceted progressive approach is equipped to handle. The increase in IoT adoption gives birth to a larger scale of threats. One critical threat that

Figure 3. Projected IoT Trends



will arise with the increase of IoT adoption is the threat caused by interdependence. The growth in the number of IoT devices being used means that interactions between devices becomes more complex. The more complex the interactions the less need there is for human involvement. IoT devices will not only communicate to each other explicitly but instead can be controlled by other conditions using services like IFTTT (if this then that). For example, home devices such as a smart smoke detector can be set to perform a certain action in response to another action. For example, if a smart smoke alarm is triggered then the smart door will automatically unlock. This smoke alarm detection and door opening scenario is a depiction of how many IoT devices are reliant on one another to function.

While this interconnectivity and common if this then that interdependence can prove to be4 convenient it is also one of the biggest threats. As IoT adoption increases and inevitably with interdependence this will also lead to the inevitable exploitation of devices within the same IoT ecosystem. The biggest threat of this interdependence is the exploitation opportunity. While target devices or systems might not be easily comprisable, an attacker could easily change the behavior of other devices within that ecosystems to achieve their aims. The attacker would be successful as the IoT devices in the ecosystem are interdependent and rely on one another meaning the siege and control over one device can lead to the demise of the rest of the dependent devices, ultimately creating an easy way for an attacker to bypass the difficult security mechanisms surround the target and instead infiltrate via interconnected device.

Another major security challenge that will result from increased IoT adoption is an increase in IoT devices without fewer safety checks. As IoT continues to grow in adoption and popularity especially amongst the business sector for its advantages in data optimization, inventory management, efficient operation and more, fewer security safety checks can be expected. As manufacturers push IoT device production to meet the demand for these devices, fewer security considerations will prove to cause substantial harm down the road for businesses. As the lack of incorporation of built-in security mechanisms on IoT devices already an ongoing issue, this will only become more severe as IoT demand grows especially in the business sector due to IoTs business optimization appeal and know advantageous.

The adoption of more IoT devices in the future also presents more data privacy and security concerns. More IoT devices means more connections to the internet, and more connections to the internet means more vulnerability to security breaches in forms such as hacking and phishing. Frequent data leaks from social media also raises earnest concerns. More IoT devices cause for a greater IoT ecosystem and ultimately adds to the exploitation potential and the potential of unauthorized data access. Unauthorized data access challenges intensify as attackers are more equipped to evade4 major security mechanisms and bypass these controls on major targets by accessing other dependent devices which inevitably results in the access to the major target and the vital data within the major target.

These increased IoT adoption and the challenges that un parallel to it will continue to expand and become more complex with time. Only a dynamic security architecture can withstand the new and complex challenges that can result over the course of time. A dynamic security infrastructure as opposed to that of a passive infrastructure will be better equipped to address new challenges. A dynamic security infrastructure will be multifaced and flexible. All layers of the infrastructure will be able to be modified and adapted to meet new security needs. In contrast to a dynamic infrastructure, a passive infrastructure would prove insufficient and would only suit for the legacy IoT systems if which it was originally designed to secure.

The atmospheric IoT approach fits the criteria of a dynamic security infrastructure as it is equipped with layers that entail the necessary security mechanisms needed for the current most prominent IoT threats. The atmospheric approach is not however stagnant in nature and can adapt and advance with IoT technology as all layers can be modified, adapted, and deleted as challenges evolve. Gradual changes to this approach can be made over time after common IoT trends are heavily monitored and reliable predictions can be made on future threats. The results gathered from analysis of IoT threat trends will aid organizations in their adaptations to the current security infrastructure. The atmospheric

approach is designed in such a way that will allow for modifications and additions the existing layers that will only create more depth in security measures surround IoT.

CONCLUSION

Implementation and Change Management

The implementation of the atmospheric IoT approach must be fully implemented into an organizations business plan. The atmospheric approach must be just as much a part of the business plan as the rest of the business proceedings. In order the implementation of the multi-face atmospheric approach to be completely successful it is crucial that it is not an after thought and is instead built into the businesses IoT implementation framework. Consideration and early application of the atmospheric approach is critical to its success and the continued security of business IoT infrastructure.

To assess the successes of the atmospheric approach implementation there are several activities that may be enacted to take on the hacker's perspective and test your infrastructure readiness. You can test the approaches readiness by attempting to attack each layer. Start with initiate any set of general threats such as data theft attempts, and social engineering attacks, in doing so you will test your threat detection readiness and validate the threat detection layer efficiency. Next, you can pull inventory on IoT devices and monitor the updates taken place on each device to ensure they are current and up to date. Upon monotint these devices if one device is found to not have been updated then you have found a vulnerability at the routine update layer and thus must enforce said updates to prevent exploitation of this vulnerability. To further test your approach, you will want to attempt to bypass certain security controls such as authorization and authentication controls. If said controls can be bypassed, then an organization must re-assess its readiness in strong security controls layer. An organization will need to also test encrypted communication protocols, this calls for ensuring proper transport layer security. Attempts to intercept usernames, and passwords or use session data to impersonate those logged in to control devices would be a great way for an organization to think like a potential attacker and test the encrypted communication layer.

The next evaluation of successful implementation involves maintaining a record of all trained organization employees on secure IoT user practices such as authentication practices and proper device management. This evaluation will evaluate the informed user practices layer. To evaluate the effectiveness of implementation and ensure the device management layer is in motion, logs of all connected devices can be maintained and routinely audited to account for all devices. To test the monitoring of IoT applications ecosystem layer penetration tester must attempt to access devices within the ecosystem. To test the traffic authentication layer is to make sure that testers cannot gain access to the network without the authorized ticket or token. Finally, the network security layer can be tested by attempts made by penetration testers to access the network and if neural network detection is functioning appropriately.

Once each atmospheric layer is tested and the successful implementation has been complete. The organization can implement some general change management plans to ensure that the approach is best supported and maximum efficiency of the approach can be achieved. Some general change management practices that should be incorporated include assessing the response of the individuals most affected by the changes in security control mechanisms, communication of change efficiency and findings to key stakeholders and the organization as a whole, and implementation of a change model to ensure a balanced and well planned change management design that an organization can utilize alongside the approach implementation to monitor success and document room for improvement in certain layers based upon implementation success results.

The rapid growth of the internet of things and the widespread adoption of the technology continues to draw urgency to addressing IoT security threats prior to IoT infrastructure deployment. The deficient security infrastructure in place an lack there of currently for IoT is an increasing concern. To remedy

current insufficient IoT security mechanisms in organizations and to make up for the mechanisms that have been yet to be deployed, a strong and dynamic approach must be initiated. The strong and dynamic approach that can meet the current security needs is also equipped to adapt and evolve with the new technologies that surround. Upon extensive research and compromission of thematic literature I have been able to consolidate various IoT security methods that combat the most prominent IoT security threats and present them the atmospheric approach. This atmospheric approach equipped to counteract the most prominent threats that plague IoT. These threats include denial of service attacks, spoofing, intrusion, malware, eavesdropping, network layer attacks, and security breaches. Each prominent threat is counteracted with a security layer of the atmospheric approach and in doing so the approach satisfies the necessary security objectives of confidentiality, integrity, availability.

Not only does the atmospheric approach to IoT security meet the core objectives of confidentiality, integrity, availability but it also proves to be a dynamic and flexible structure that can evolve and meet the new security needs that arise with the development of new IoT technologies. IoT security trends can be routinely monitored, and the appropriate additions can be easily applied to the approach as new concerns present.

RESEARCH LIMITATION

The research limitation is the scope of discussions. The future research in IoT security and my future research in this area specifically are ongoing. Thus, due to the progressive nature of the topic and the ongoing changes in concerns, challenges, and practices, my current research discussion is limited to the data and information currently collected through extensive literature review and assessment of necessary IoT infrastructure security mechanisms. The scope of our discussion is limited to our developed security approach and the atmospheric IoT security approach developed around the premise of the most common IoT threats and security shortcomings currently surrounding organizational IoT infrastructure. As time continues and new threats encompass IoT, new discussions will be prompted. Expected ongoing IoT security challenges include insecure interfaces, insufficient data protection, poor device management, gaps in IoT skills, lack of regular patches and updates, and weak update mechanisms. These ongoing security challenges may evolve into more complex challenges as new factors may influence the severity of these ongoing concerns. Thus, projected IoT security challenges are expected to intensify and become more complex and be accompanied by all-new challenges, all of which will prompt new discussion and the advisement of modification to my current IoT security atmospheric approach.

FUTURE RESEARCH

Although future challenges in IoT security are unknown, we can anticipate future challenges through monitoring and analysis of IoT threat trends. Over time, monitoring these IoT security threats will determine the future details and focus of my ongoing research on the topic. Some anticipated and growing threats include AI in IoT threats and deep fakes for IoT threats. Based on these IoT threat predictions, one can say that our future research will be based on the predicted IoT threats AI in IoT threats and deep fakes for IoT threats. Our future research involves the modification to my proposed atmospheric IoT approach. New layers, additions, and adjustments to existing atmospheric layers will be incorporated because of up-and-coming threats that will prompt the re-assessment of my research to meet current security challenges.

Although the flexible design of my approach allows for and anticipates the modification of security layers to address new threats, it is still centered around current threats. My strategic IoT atmospheric approach is robust in design as it is designed to adapt to new threats and concerns; the current threats and my current approach limit the scope of my discussion. However, these limitations

also outline the premise of my future research on the topic, as my future research will be centered upon new threats and new developments in IoT technology.

For future IoT security threats I highly recommend that organizations incorporate and continue to incorporate flexible and multifaceted IoT security approaches. Multifaced IoT approaches will provide the most comprehensive security possible for the IoT infrastructure. The flexibility of the approach will aid the organization in aligning security practices with new threats that arise. Without crucial factors such as a comprehensive approach and approach flexibility the organization would surely be at a significant disadvantage. Thus, it is with great urgency that I recommend implementations of strategic, flexible, and comprehensive IoT security infrastructure now and in the future.

REFERENCES

Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An iot perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22. doi:10.3390/jsan8020022

Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A., & Shekhar, S. (2018). Continuous security in iot using blockchain. *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. doi:10.1109/ICASSP.2018.8462513

Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer iot: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, *9*(2), 17–25. doi:10.1109/MCE.2019.2953740

Bica, I., Chifor, B., Arseni, Ș., & Matei, I. (2019). Multi-Layer IoT security framework for ambient intelligence environments. *Sensors (Basel)*, *19*(18), 4038. doi:10.3390/s19184038 PMID:31546782

Bugeja, J., Vogel, B., Jacobsson, A., & Varshney, R. (n.d.). IoTSM: An End-to-end Security Model for IoT Ecosystems. Reading.

Bull, P., Austin, R., Popov, E., Sharma, M., & Watson, R. (2016). Flow based security for iot devices using an SDN GATEWAY. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE. doi:10.1109/FiCloud.2016.30

Castillo, A., & Thierer, A. D. (2015). Projecting the growth and economic impact of the internet of things. SSRN *Electronic Journal*. 10.2139/ssrn.2618794

Chart, diagram & visual Workspace Software. (2019, July 10). Creately. https://creately.com/

Damghani, H., Damghani, L., Hosseinian, H., & Sharifi, R. (n.d.). *Classification of Attacks on IoT.* Iran University of Science and Technology.

Eutelast, E. (n.d.). *5 trends Proving IoT is the future.* Eutelast. https://www.eutelsat.com/en/blog/5-trends-proving-iot-is-the-future.html

Ivan, C., Vujic, M., & Husnjak, S. (2016). Classification of security risks in the iot environment. *DAAAM Proceedings,* (pp. 0731-0740). DAAAM International. doi:10.2507/26th.daaam.proceedings.102

Khan, M. A., & Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. doi:10.1016/j.future.2017.11.022

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. *2012 10th International Conference on Frontiers of Information Technology*. IEEE. doi:10.1109/FIT.2012.53

Network Security. (2014). Lack of security in internet of things devices. (2014). *Network Security*, *2*(8), 2. doi:10.1016/S1353-4858(14)70075-3

Lampropoulos, G., Siakas, K., & Anastasiadis, T. (2018). Internet of Things (IOT) in industry: Contemporary application domains, innovative technologies and Intelligent Manufacturing. *International Journal of Advances in Scientific Research and Engineering*, *4*(10), 109–118. doi:10.31695/IJASRE.2018.32910

Liu, C., Zhang, Y., & Zhang, H. (2013). A novel approach to iot security based on immunology. *2013 Ninth International Conference on Computational Intelligence and Security*. IEEE. doi:10.1109/CIS.2013.168

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (n.d.). *IoT Standardisation - Challenges*. Perspectives and Solution.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). Iot privacy and security: Challenges and solutions. *Applied Sciences (Basel, Switzerland)*, *10*(12), 4102. doi:10.3390/app10124102

Vailshery, L. (2016, November 27). Number of IoT devices 2015-2025. *Statista.* https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Vyas, D. A., Bhatt, D., & Jhaq, D. (2015). *IoT: Trends*. Challenges and Future Scope.

Works, D., & -. (2020, June 08). *Practical cryptography for the internet of things*. IoT For All. https://www.iotforall.com/cryptography-for-io

Writer, G. (2019, June 27). Iot statistics and facts - infographic. *Disruptive Asia*. https://disruptive.asia/iot-statistics-and-facts-infographic/

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, *35*(5), 41–49. doi:10.1109/MSP.2018.2825478

Xu, T., Wendt, J. B., & Potkonjak, M. (2014). Security of iot systems: Design challenges and opportunities. *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. doi:10.1109/ICCAD.2014.7001385

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and Privacy: New THREATS, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606–1616. doi:10.1109/JIOT.2018.2847733

Zúquete, A., Gomes, H., Amaral, J., & Oliveira, C. (2019). Security-Oriented architecture for MANAGING Iot deployments. *Symmetry*, *11*(10), 1315. doi:10.3390/sym11101315

APPENDIX A

Challenges of IoT Interdependent Behaviors

The equation below is an example of the dangers of interdependent IoT devices specifically in the form of a Device Hijacking Attack Example of a Joy Link Protocol.

The equation demonstrates the tunneling effect of the Joylin protocol that illustrates how attackers can exploit security vulnerabilities and work together to continue exploit victims by operating thorough the same channel. Finding these protocol vulnerabilities that attackers take advantage of is difficult as every network protocol has differences with others and thus extensive digging out of crucial security problems.

Device Hijacking Attack Example of JoyLink Protocols: Forge victim device MAC to register
+ respond communication key & deviceid+ send key & devicceid to the device of the victim
= binding victim device to attacker cloud account

APPENDIX B

The list in table 2 includes other notable IoT security threats to anticipate a possible increase in. These threats, while not the most prominent they are still mentionable. All the threats below are low to medium threat levels and thus do not fit the mold for the most urgent and prominent IoT security threats. Thus, the flowing threats were not listed in Table 1. Instead, a separate brief table for these low threat level IoT threats is formatted below.

Table 2. Low-Level IoT Threats

Threat Type	Threat Level
Range extension (enables the option to extend the range for a case of execution attacks)	Low
Obfuscation (allows for hiding of attacker identity)	Low
Surveillance (enables information gathering on the user.	Low

M'Kaila Clark is an Assistant Professor at Onondaga Community College in Syracuse, New York, for the Health Information Technology department. She graduated with her Master of Science in Information Technology and a concentration in cyber security from Empire State College. M'Kaila Clark's work involves helping students learn and synergize healthcare and informatics technology knowledge. She plans to continue building awareness on the continued intersectionality of health and information technology amongst her students.

Lila Rajabion received her doctoral degree in Management of Information Technology from Lawrence Technological University and also holds a MS in Computer Information systems from University of Detroit Mercy. She holds two undergraduate degrees in Computer Science and Psychology from University of Windsor, Canada. Lila has over 15 years of professional experience in various dimensions of Information Technology combined in the academia, and the private sectors. She also has a significant work experience in providing leadership in the areas of systems analysis & design, cyber security, enterprise software application development, and IT project management for local and "global" projects. Dr. Rajabion is a co-founder of ITC4BIZ and providing IT consulting services to worldwide customers.