Artificial Intelligence and Machine Learning within the context of Cyber Security used in the UK SME sector

Nisha Rawindran, Ambikesh Jayal and Edmond Prakash

Contents

1 Introduction

This extended abstract contains the finding of two broad studies. Each study examines ideas of the challenges arising from aspects of cyber security in using Intrusion Detection mechanisms together with Artificial Intelligence (AI) and Machine Learning techniques in the protection of small and medium enterprises (SMEs) in the UK, for its operations and commercial environment.

Both papers explored intrusion, detection, and prevention methods as a priority in the realisation of keeping their data secure and safe with the integration of real-world objects within the internet such as Machine Learning techniques and AI. Both papers go on to then establish the various methods of improving its cyber security.

2 Intrusion, Detection and Prevention

The first paper was an experimental scenario in which the Intrusion, Detection and prevention model was compared, and the views of the SME examined. The study looks at the various approaches in identifying ways to detect and protect any intrusions coming into the network and what operating devices would help in this process.

This paper explored the understanding in trying to protect the data and how government policies and procedures such as the General Data Protection (GDPR) of the UK, could assist towards this process. This study also examined the impact of how threat levels of attacks such as Ransomware, Phishing, Malware, and Social engineering amongst others, were compared between the Open-Source code, such as SNORT and pfSense, and Commercial Network Intrusion Detection (NIDs) such as Cisco. There were three different NIDs and their features were compared. It was concluded that whilst SNORT and pfSense were free to use from the Open-Source Market, it required a certain level of expertise to implement and embed the rules into a business solution. It was also noted that Cisco, due to their engineering expertise and their position as market leaders in the industry, were able to embed these free rules and use it to their advantage. What emerged from this study was how businesses and organisations with the help of government policies and processes, needed to work together to combat these hackers, malicious actors and their bots, and manage and stay ahead of the game.

The paper discusses various AI and Machine Learning approaches such as Signature based models and Anomaly based rules used by these devices to combat these attacks. Signature based models could

only detect attacks that were known whereas anomaly-based systems were able to detect unknown attacks. Anomaly-based NIDs made it possible to detect attacks whose signatures were not included in rule files. Unfortunately, due to the maturity of Anomaly NIDs, the costs were still very high to run and required computing power that was unrealistic in the SME environment. Anomaly based NIDs whilst still in its infancy, required a deeper analysis and future study. This study provided perspectives on better comparisons and relative conclusions and how it was important to explore further both the empirical as well as in scenario analysis for different dimensions the nature and context of cyber security in the current world of internet and cyber connections. The first study leads aptly on to the second study.

3 AI and Machine Learning

The second paper examines how AI and Machine Learning techniques have become vital in the growth and dependencies of these SMEs in the UK in their operations and commercial environment. This study took on an initial look at success stories from big technology companies such as Amazon, Google and Facebook, in their use of Machine Learning techniques for their cyber security. The methodology adopted in this second study focused on structured survey questions on a selected sample number of respondents and directed its questions to the SMEs management, technical and non-technical professionals. The study found that awareness of Machine Learning and its uses is still on a learning curve and yet to be defined.

Whilst Machine Learning produced cyber security challenges, this study deducted and quantified its examples and showed a strength it is the SMEs perception and awareness towards Machine Learning. The study revealed that SMEs had the appropriate Cyber Security Packages in place but not necessarily aware of its full potential. It also showed that management and their technical knowledge was not perhaps in depth to the level of Machine Learning and its algorithms. They were familiar of the security and safety these packages gave to their company; however, they could not identify further the technical aspects of these software. They were merely recommended these solutions from suppliers however the study acknowledged that management wanted to learn more and have a better understanding of AI and Machine Learning integration. The expertise of the IT team were found to be paramount on how Machine Learning was going to be used in the future. The second study also took priority of GDPR and awareness towards the regulation of cyber security.

From both studies, the initial idea of using an Intrusion, Detection and Prevention method, from either a commercial or open source to protect the data of the SME, comes with the knowledge of Machine Learning and AI. Both studies reflected on these results whereby Machine Learning through Anomaly detection proved to be more effective in its zero-day detection than that of Signature based in its effectiveness towards Cyber Security and their adoption within the UK SMEs. Both papers recognised an important gap that needed to be fulfilled by perhaps more Opensource and voluntary participants from knowledge of the community to keep future proofing these devices. Both papers also highlighted the importance of funding gaps that could be fulfilled by the government to support SMEs in the form of grants, subsidies, and similar financial assistance through various public sector policies. Both studies also recognised the awareness and training importance for all management and their staff to understand the basic and perhaps advanced appreciation of Cyber security through the eyes of Machine Learning and AI. Whilst technology giants as mentioned above might lead the path in its implementation of Machine Learning and cyber security through its many variations of intrusion, detection and prevention methods, it is through these firms that will set precedence and bring awareness down to SME level and the importance of Machine Learning in keeping our cyber world safe.

4 SMEs - The Way Forward

The final message is for SMEs to raise their game in the awareness of cyber-security and Machine Learning and AI as the way forward in growing their business in a safe and secure way in protecting their data.