**Claim:**

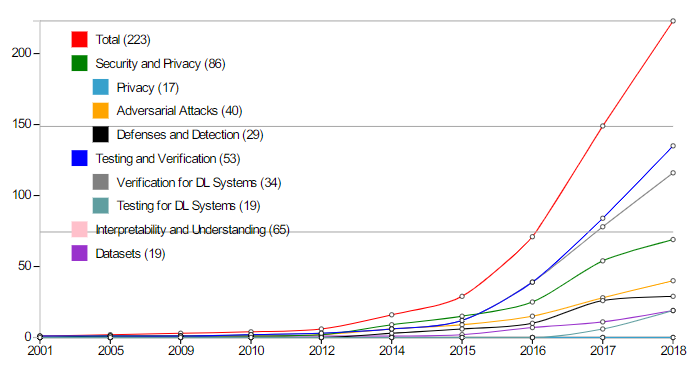
Software Engineering Quality Assurance can pave the path for the software engineering community towards addressing the pressing industrial demand for secure intelligent deep learning applications. (Aristotelian or Classical Argumentative Essay)

Note: First submission point is 17.I updated my comments according to the feedback. First used claims then evidences in the from of ethos, pathos, logos. And Referencing styles also updated publications are added.

**Software Engineering Quality Assurance on the Path to the Pressing Industrial Demand for Secure Deep Learning Applications**

Over the past decades, deep learning (DL) systems have achieved tremendous success and gained great popularity in various applications, such as intelligent machines, image processing, speech processing, and medical diagnostics. According to Secure Deep Learning: A software quality assurance perspective article published in 2018, “Deep neural networks are the key driving force behind its recent success, but still seem to be a magic black box lacking interpretability and understanding. A plethora of studies have shown that the state-of-the-art DL systems suffer from defects and vulnerabilities that can lead to severe loss and tragedies, especially when applied to real-world safety-critical applications” ( as cited in Lei M., Xu J., Minhui X., Qiang H., Sen C., B. Li, Yang L., Jianjun Z., Jianxiong Y., Simon S., 2018 ). This brings up many open safety and security issues with enormous and urgent demands on rigorous methodologies and engineering practice for quality enhancement. Comments like this and the obvious hysteria which is becoming more and more important with the widespread of deep learning applications use in intelligent platforms and smart devices leaded SWEBOK authors to deep dive into the subcategory of software quality management process and software quality management assurance. This essay will advance the claim that software engineering quality assurance can pave the path for the software engineering community towards addressing the pressing industrial demand for secure intelligent deep learning applications both with the supportive and opposite ideas with evidences.

As mentioned in the above, with the widespread deep learning applications use and change in time and access of the internet, everything has changed its nature especially the field of information technology with increased usage of data-driven software has impacted a lot. One of the strongest assertions for the software engineering quality is that software engineering quality management and software quality assurance can provide standards that are beneficial to tackle the protection of sensitive data of users and other privacy challenges securely and safely. Strong evidence that shows why it is getting more critical to provide software quality assurance for data-driven deep learning applications by performing activities is stated in the Secure Deep Learning Engineering: A Software Quality Assurance Perspective paper published in 2018 again as, “The latent software quality and security issues of current DL systems, already started emerging out as the major vendors, rush in pushing products with higher intelligence (e.g., Google/Uber car accident [3, 4], Alexa and Siri could be manipulated with hidden command [5]. A DL image classifier with high test accuracy is easily fooled by a single-pixel perturbation [6])”. However, current DL system development still lacks systematic engineering guidance, quality assurance standards, as well as mature toolchain support. Deploying such cocooned DL systems to real-world environment with-out quality and security assurance leaves high risks, where newly evolved cyber- and adversarial-attacks are inevitable” ( as cited in Lei M., Xu J., Minhui X., Qiang H., Sen C., B. Li, Yang L., Jianjun Z., Jianxiong Y., Simon S., 2018 ). Also, the number of high demand in the publications about more secure DL applications which proves that we need to perform activities in the software quality assurance in the libraries can be observed year by year and classified by their topic in Figure 1.0.



*Figure 1.0. The accumulative number of selected publications over years (Secure Deep Learning Engineering: A Software Quality Assurance Perspective, 2018)*

According to Figure 1.0., there is an immediate raise after 2015 in publications about security and privacy. The reason why it has the highest rank among the other topics is that every type of DL system has several different kinds of problems with data security since they are implementing real-life applications. This is also stated in Security and Privacy Issues in Deep Learning paper published in 2019 as, “Development of deep learning (DL) algorithms have transformed the solution of data-driven problems in various real-life applications, including the use of large amounts of patient data for health prediction services [Shickel et al. 2017], autonomous security audits from system logs [Buczak and Guven 2016], and unmanned car driving powered by visual object detection [Ren et al. 2015].( Bae H., Jang J., Jung D., Jang H., Ha H., Yoon S., 2019)”. According to the U.S. Department of Homeland Security, the Software Quality Assurance (SQA) project develops tools and techniques for analyzing software to identify potential security vulnerabilities associated with critical national infrastructure and networks (Official website of the Department of Homeland Security, 2019). Therefore, since software quality management and assurance in real-life applications which has deep learning background can constitute secure and safe environment for sensitive data of the users, it can pave a secure data usage path for the software engineering community towards addressing the pressing high industrial demand; also another referring idea for this thesis is user data privacy is an important dimension of software quality which attempt to improve secure DL applications.

Another strong argument under this general thesis is software quality standards and assurance activities provide secure maintenance and adaptation after deployment of the DL applications. Software quality assurance is concerned with the problems of ensuring and demonstrating that software will satisfy the security needs and requirements of those who procure them in the previous argument. These needs and requirements may cover not only how well software works now, but also how easy to fix if it does go wrong, or how much those DL applications are secure when it comes to adaptation to new requirements that were raised by the security leaks in the system. To satisfy this healthy maintenance and easy adaptation of DL product cycle Software quality assurance proposes to spend much more time in the verification and validation process. According to the Software Quality Assurance book published in 1988 by NASA, “The two processes are complementary: each is effective at detecting errors that the other will miss, and they are therefore usually employed together. And it is usually cheap and simple to correct a coding bug caught during unit tests, and it is usually equally simple and cheap to insert a missed security requirement that is caught during system requirements review in AI applications ( Rushby J., 1988)”.For this process we can also give very basic applications from the real-life, when there is a new software update in customers’ smart device that is using DL background, they want it to be easily an securely adaptable to the new software and reliable. And the following sentences from the paper called Quality Assurance for Data Analytics published in 2019 is a good evidence to this need: “ Quality Assurance (QA) related activities are proven to be beneficial because it gives a confidence about the completion of requirements and needs that a user expect from a system, it can be the quality of product or it may be the accessibility and reliability, accessibility and reliability are just two qualities of systems, there are many more suggested by different experts( Kumar R., Subhash B., Fatima M., Mahmood W., 2019)”. Therefore, these needs and requirements related to security may cover not only how well the DL software works now, but how well documented it is, how easy to fix if it does go wrong, how adaptable it is to new requirements, and other attributes that influence how well it will continue to satisfy the user’s needs in the future, means software quality assurance from the verification & validation perspective also can pave the path for the software engineering community towards addressing the pressing industrial demand for secure intelligent deep learning applications.

On the other hand, quality and quality assurance of the DL code may not always be secure. According to G. Mcgraw, “A central and critical aspect of the computer security problem is a software problem. Software defects with security ramifications—including implementation bugs such as buffer overflows and design flaws such as inconsistent error handling—promise to be with us for years (G. McGraw, 2004)”. All too often, malicious intruders can hack into systems by exploiting software defects [11]. Though these data points are clear indications, the quality software is not yet synonymous with secure software. There are numerous reasons. For example, because of the changing digital economy means speed rules. This means, when the software is key to an organization’s ability to compete and innovate, security can be a tough sell. In the developing world today, functionality and delivery speed outweigh all else – including security. Enterprises simply can’t stay ahead of the competition without getting new features out fast. With that kind of pressure and speed, security typically falls by the wayside. And when the security of the software falls by the wayside and software quality management process fails, there may be some undesirable results. For example, according to the Alan M. Davis and Dean A. Leffingwell, “Over 30% of all software projects are canceled before completion; Over 70% of the remainder fail to deliver expected features; The average project runs 189% over budget and overshoots its schedule by 222% ( Alan M. Davis and Dean A. Leffingwell, 1995).In the worst case, if the software quality requirements don’t meet there may be risky security problems. Some of them are stated in the Security and Privacy Issues in Deep Learning paper published in 2019 as, “If a DL model causes mispredictions or misclassifications due to malicious external influences, then it can cause very large difficulties in real life. Moreover, training DL models involve an enormous amount of data and the training data often includes sensitive information. Therefore, DL models should not expose the privacy of such data (Bae H., Jang J., Jung D., Jang H., Ha H., Yoon S., 2019)”. Thus, when sometimes even when the software quality assurance requirements said to be met if the processing speed was high then that means that there may be poor software quality requirements were included in that DL applications which then leads to security problems and leaks.

In conclusion, with technology advances in recent years, security problems become more important. Security measurement and monitoring help system developers to design and assure systems with high software engineering quality management. And the subcategory of the software engineering quality management, software quality assurance can be a boon to the software engineering community towards addressing the pressing industrial demand for secure intelligent deep learning applications cause with the development of machine learning (ML), expectations for artificial intelligence (AI) technology have been increasing daily. Protecting sensitive data of the users when they are using DL applications and adaptation to new requirements in the DL application life cycle are playing supportive roles in the software quality assurance process. We can continue to spend countless amounts of time to dive into the software engineering quality and its’ subcategories to deploy DL applications with high security.

**References**

1. Lei M., Xu J., Minhui X., Qiang H., Sen C., B. Li, Yang L., Jianjun Z., Jianxiong Y., Simon S. (2018), Secure Deep Learning Engineering: A Software Quality Assurance Perspective. *Cornell University Press, 2018.*

<https://arxiv.org/abs/1810.04538>

1. Kumar R., Subhash B., Fatima M., Mahmood W. (2018), Quality Assurance for Data Analytics. *Article Published in International Journal of Advanced Computer Science and Applications(ijacsa), Volume 9 Issue 8, 2018.*

<https://thesai.org/Publications/ViewPaper?Volume=9&Issue=8&Code=ijacsa&SerialNo=21>

1. Ziegler, C., (2019),GoogleAccident:AGoogleself-driving car caused a crash for the first time , *California DMV*. https://www.theverge.com/2016/2/29/11134344/google-self-driving-car-crash-report
2. Metz, C., Uber Accident: After Fatal Uber Crash, a Self-Driving Start-Up Moves For-ward(2018), *NewYork Times Press.* https://www.nytimes.com/2018/05/07/technology/uber-crash-autonomous-driveai.html
3. Metz, C., (2018),The New York Times: Alexa and Siri Can Hear This Hidden Command. You Can’t. *NewYork Times Press.* (2018),https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html
4. Bae H., Jang J., Jung D., Jang H., Ha H., Yoon S., 2019, Security and Privacy Issues in Deep Learning, *Cornell University Press.*<https://arxiv.org/abs/1807.11655>.
5. Official website of the Department of Homeland Security., 2019. <https://www.dhs.gov/science-and-technology/sqa>
6. Rushby J., (1988, p.5-6) ,Quality Measures and Assurance for AI Software. *Nasa Contractor Report 4187.*

<https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19880020920.pdf>

1. G. McGraw,( 2004, p.80-83 ), Software Security, IEEE Security & Privacy. *IEEE Security & Privacy (Volume: 2 ,Issue: 2 , March-April 2004 ).*

<https://ieeexplore.ieee.org/document/1281254>

1. G. Hoglund, G. McGraw, Exploiting Software: How to Break Code, 2004. *Gary McGraw, Ph.D.CTO, Cigital.*

<https://www.usenix.org/legacy/events/sec04/tech/slides/mcgraw.pdf?ref=driverlayer.com/web>

1. Alan M. Davis and Dean A. Leffingwell (1995), Using Requirements Management to Speed Delivery of Higher Quality Applications.*ResearchGate.net Publications.*

<https://www.researchgate.net/publication/2385516_Using_Requirements_Management_to_Speed_Delivery_of_Higher_Quality_Applications>

1. Shickel B., Tighe P., Bihorac A., Rashidi P. (2018), Deep EHR: A Survey of Recent Advances in Deep Learning Techniques for Electronic Health Record (EHR) Analysis.*Cornell University Press.*

<https://arxiv.org/abs/1706.03446>

1. Guven E., Buczak A. (2016), A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE xplore Digital Library.*

<https://ieeexplore.ieee.org/document/7307098>