Cybersecurity : Analysis of Attack forecasting

Tomás O'Malley, *BSc Software Development (Honours), GMIT*

***Abstract*—Abstract—This review will tackle and review the current state of cyber-security and forecasting models developed. Computers have become the foundation and backbone of how we communicate, interpret data, and push forward today. Over the last decade advancements in information technology from the large consumer use of personal computers and smartphones have led to increased demand for tight security solutions in areas like e-commerce, social media sites, and including banking. Today ina society where big-data companies hold so much of our valueable data using cloud computing, IoT security, companies must provide high-level security to prevent attacks on their customers and income. I later in this review, discuss the current state of cyber security forecasting and future gaps/advancements through the use of deep learning and artificial intelligence.**

***Index Terms*—cybersecurity, information technology, cloud-computing, attack-forecasting, deep learning**

I. Introduction

A. A Brief History of Cyber Security

As far back as the early 1970s cybersecurity has been a prevailing topic in society beginning with the ARPANET (The Advanced Research Projects Agency Network)[1]. By nature humans and their systems are flawed, threats such as Malware, Phishing, Trojans, DDoS still exist today. Data breaches such as the Bright Researchers have been brewing algorithms to prevent cybercrimes (Identity fraud, card payment data). Information technologies and the introduction to Tim Berners Lee Wide Wide Web in 1989 added a new layer of threats for governing groups using AV technology and firewalls to force restrictions from specified network access. New obstacles include the introduction of ransomware in 2017 forcing windows users to pay to gain access to their device. As described by the multinational company in the year of 1991 [2]" Less than a year after SAM and Norton Utilities came together, Symantec launched Norton AntiVirus™ for PC — its very first antivirus software for consumers" continue to provide security options in 2020. Underneath is a Gantt chart provided.

B. Current state of security

When viewing cybersecurity there are three main trends for gateways for malicious attacks CNA-Computer Network Attack, CNE-Computer network Exploitation, and CNI-Computer Network influence, Cyber Crimes are prevailing and [3] Europol states that cyber crimes have now become more common than street crime. Research firm Juniper claim [4] "IoT connections to grow 140 percent to hit 50 billion by the year 2022, as edge computing accelerates ROI".Due to the covid-19 pandemic (2020) currently employees globally are working remotely to maintain and improve fault tolerance services. New data shows the pandemic will benefit but deeply challenge cybersecurity and how companies fund services. Microsoft has issued a statement [5] "Technology alone cannot keep pace with the threats and demands facing businesses and their largely remote workforces."

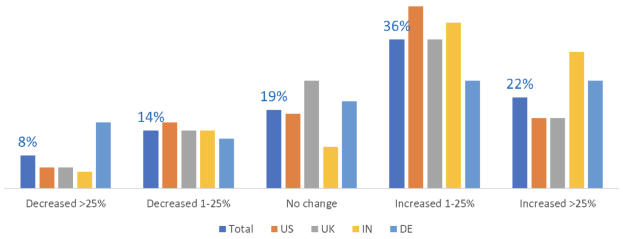

Fig. 1. Fig.1 2020 pandemic Multinational budget changes

II. Solutions

A. The Definition of Cyber Security

Cybersecurity is described in websters dictionary as " measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack". It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories. From military research, a methodology referred to as cyber situational awareness is applied. One of the most widely used definitions of situational awareness is by Endsley in their paper [6] "Perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in near future."

As of 2018, there have been 80,000 cyberattacks a day, The key is for Big-data companies to develop a threat model in which these threats can be pre-determined and dealt with in advance.

1) Attack Forecasting: Attack forecasting in principle can be compared to the benefits of the weather forecast so we can prevent/dodge an unwanted position. Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example of quantum cryptography is the quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. As touched on by Martin Husak [7] we must to document the behavior of the attackers and establish a description of an attack for later use when incorporated into a realistic model. An adaption commonly used is the "Hidden Markov Models states for prediction" outlined in Alireza paper [8]. By observing and analyzing the attempts we can forecast future events as described by [**hmmn**] "allows us to talk about

both observed events Hidden Markov model that we think of as causal factors in our probabilistic model of observable events".[9] The Hidden Markov model was first used in speech recognition and has been successfully applied to the analysis of biological sequences since late 1980 in computing.

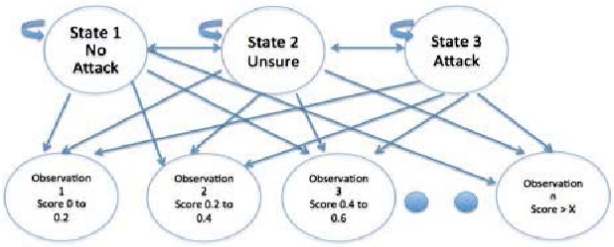

Figure 3 The model that detects anomaly from big data

Fig. 2. Fig 2 provides an application of a The Hidden Markov Model.

The model focuses on three states.

- State 1 No Attack : state in which the service has not been attacked.
- State 2 Unsure : state in which there is potential of further attack.
- State 3 Attack : state in which the organisations services have experienced unexpected/unusual traffic.

2) Types of Attacks : Cyber attacks have been a serious computing issue since the dawn of computing from the floppy disk to over networks.There are many methods and classifications of threats for online security. Underneath I will evaluate the most common threats faced by governed data and consumer data.Documentation from CSI Computer Crime Security Survey [10]

1) Virus: Alison Grace for Norton security [11] describes a virus as an "A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. "
2) Phishing: As defined by websters dictionary ": a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly".Prime examples of phising can be found in your email client sometimes in the form of spam requesting information.
3) Denial of Service (DDOS): As described by Steve Weisman team at Norton [12] "Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable."DDOS attacks take advantage off less secure architecture.

These are all prime examples of modern-day cyber threats that companies must prepare to prevent

III. Proposed Technologies

With three fundamental motivations behind Cyber Security in mind, we must then contemplate the technologies required to achieve such goals. Like its standards, cyber attack technologies have also not been completely decided on. However, some promising technologies have emerged and include; Blockchain, Model Development, and Deep Learning.

A. Blockchain

Blockchain technology enables trusted transactions among untrusted participants in the network. Incorporating the blockchain completely eliminates the need for businesses to authenticate and provide secure access to users and devices without using any password. Blockchain technologies were invented in the year 2009 created to replace flat currency and currently, there are few literature reviews due to its short introduction in security. As of last (2019) year, a paper by Salman [13] discusses "The technology started with Bitcoin, a cryptocurrency that has reached a capitalization of 180 billion dollars as of January 2018".Currently in the market their seems to be large investment and research for blockchain in digital currency and a gap in research for addition to cyber-threat and attack forecasting.

B. Big Data

Websters Dictionary defines big-data as an accumulation of data that is too large and complex for processing by traditional database management tools. Examples of sources of big data transactions are data from computer networks, telecommunication networks (BT, Verizon, finance (Fidelity, healthcare (HSE), social media (Google+), etc. The domain of Big Data Analytics (BDA) is concerned with the extraction of value from big data, i.e., insights that are nontrivial, previously unknown, implicit, and potentially useful. Seagate the multinational store 75 zettabytes(. One Zettabyte is approximately equal to a thousand Exabytes, a billion Terabytes, or a trillion Gigabytes) of data by the year 2025.

The act of accessing and storing large amounts of information for analytics has been around for a long time. By optimizing/surveying pools of data companies can try to forecast the next attempt. In A. Gheyas survey [14] He outlines The key challenges facing the insider threat detection and prediction system include unbounded patterns, It is extremely difficult to harvest the data correctly and model for the behavior to prevent attacks from the model created.

C. Develop Model

The aim is to create impact solutions rather than point fixes for large scale systems.

Xing describes the training as a model for predicting attacks In the training process, we use the mini-batch gradient descent method to compute the minimum of the objective function, which is described in Eq. (1). We use 10,000 iterations to train a network and set the penalty parameter =.001 because other parameters do not lead to any significantly better results. For each dataset, we use Algorithm 1 to compute the fitted values with varying model parameters. We select the model that achieves the minimum MSE.[15]

It is a common construction for companies to create state cycles as reviewed in the journal .

D. Deep Learning

Deep learning refers to a type of machine learning based on artificial neural networks in which multiple layers of processing are used to extract progressively higher-level features from data. As outlined by Vinayakumar the raw input can be applied towards use cases such as intrusion detection, malware classification.There a many approaches for deep learning such as Recurrent neural network (RNN) , Long Short Term Memory Networks(LSTMN's) and Self Organizing Maps (SOMs).Deep learning is incorporated into many types of security software used by both consumers and organisations.Organisations will need to train the model by using their own data set to create predictions for the possibilities of an attack to their services.

[**security**]

IV. The Future of Cyber Security

A. Emerging threats in Cyber Security

Complications and questions arise with each major development in any area of online technologies.

1) Ever Expanding Users : As of the year 2020, there are 1.69 billion users on the social media platform "Facebook" standalone. Through the ever-expanding of the used Internet of things and smart devices leads to more potential attacks to their data. Each decade a new platform succeeds the last from MySpace to Facebook. Companies must incorporate solutions to prevent intrusions on all devices such as Android, PC, Mac, and iOS.Due to the Covid-19 Pandemic Students are learning completely in a digital format vulnerable to attacks such as Phishing, Malware, DDoS (Direct Denial of Service), and Ransomware.

2) Social Engineering: Websters Dictionary defines social engineering as ": management of human beings in accordance with their place and function in society : applied social science".In recent years juggernaut company yahoo in 2013 was attacked which resulted in a breach of 3 billion accounts holding names, passwords, and card data due to the use of social engineering from an outside entity.It is very difficult to element this factor as it is entirely human dependent.

B. Possible Use Cases of Attack Forecasting in Cyber Security

In a world where Big Data becomes more sophisticated and unpredictable by the day in this section, I will define and outline the 3 possible use cases in Attack forecasting systems.

1) In Day-to-Day Life: One of the largest advantages of attack forecasting is from the user's endpoint. If Multinational-companies such as Google Microsoft, Apple successfully crack the code user downtime will be lowered and create a stronger dependence and trust for organizations and consumers. An example of a company attacked using DDOS is Sony, The attack occurred between April 17 and April 19, 2011, forcing Sony to turn off the PlayStation Network on April 20, This large outage has had dire consequences for its brand reputation and users faith in their security.

2) The Bigger Picture: The leap from current computing to the fifth generation(Quantum Computing)of computing will allow for the creation of quantum-safe encryption in cryptography.It is undeniable that user experience on many levels can be greatly improved. However, it is important to recognise the benefits of improved cybersecurity on a societal and global level.In education, one large advantage of attack-forecasting is the reduction of down times for multimedia platforms for connecting eachother. Additionally attack forecasting can provide higher reliability/dependence to pave the path for smart cities and autonomous transport .

V. Conclusion

The way we communicate and incorporate technology into both our personal lives and wider society is changing greatly with each passing year. While the technologies mentioned in this review have shown considerable potential, but there is yet much research and landmarks to overcome before attack forecasting can change Security for consumers and developers.These possibilities, coupled with the need to improve on current cybersecurity systems and our ever-increasing demand for higher 24/7 365 services no downtime and more reliable systems, will be the driving forces behind the advancements to come in the future.

References

[1] Paul DiMaggio. "Q". In: *From Unequal Access to Differentiated Use: A Literature Review and Agenda for Research on Digital Inequality** 32.8 (2002), pp. 7–8. DOI: https : / / digitalinclusion . typepad . com / digital_ inclusion/documentos/revdimaggio.pdf.

[2] a NortonLifeLock employee NortonLifeLock. "The evolution of Norton™ 360: A brief timeline of cyber safety". In: *Norton* (2018).

[3] Bo Rotoloni Wenke Lee. "Emerging cyber threats, trends and technologies". In: *Telektronikk* 101.3/4 (2016), pp. 22–23.

[4] A. L. Swindlehurst et al. "IoT Connectivity Technologies and Applications:" in: *IEEE* (2018). DOI: 3.

[5] Andrew Conway. *New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security*. Accessed on 21 Nov 2020. URL: https : / / www . microsoft . com / security / blog / 2020 / 08 / 19 / microsoft - shows - pandemic - accelerating - transformation-cyber-security/.

[6] M. R. Endsley. *situation awareness global assessment technique (SAGAT)*. Accessed on 27 Dec 2020. 1988. URL: https://sci-hub.do/https://ieeexplore.ieee.org/document/195097#.

[7] Martin Husak IEEE. *Survey of Attack Projection, Prediction, and Forecasting in Cyber Security*. Accessed on 25 Nov 2020. URL: https://sci-hub.do/https://ieeexplore.ieee.org/document/8470942#.

[8] Alireza Shameli Sendi. “Real Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Model”. In: *IEEE Journal on Selected Areas in Communications* 32.6 (2012), pp. 312–313.

[9] Monica Franzese. “Hidden Markov Models”. In: *IEEE Communications Magazine* 52.1 (2014), pp. 1–2. DOI: https://sci-hub.do/https://www.sciencedirect.com/science/article/pii/B9780128096338204883#.

[10] CSI Director Robert Richardson. *2008 CSI Computer Crime and Security Survey*. URL: http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf.

[11] Alison Grace Johansen. *What is a computer virus?* URL: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

[12] Steve Weisman. *What is a distributed denial of service attack (DDoS) and what can you do about them?* URL: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html.

[13] World Health Organisation. *Security Services Using Blockchains: A State of the Art Survey*. Accessed on 26 Nov 2020. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8428402.

[14] Iffat A. Gheyas. *Detection and prediction of insider threatsto cyber security: a systematic literaturereview and meta-analysis*. Accessed on 17 Oct 2017. URL: https://www.researchgate.net/publication/307527489_Detection_and_prediction_of_insider_threats_to_cyber_security_a_systematic_literature_review_and_meta-analysis.

[15] Xing Fang. *A deep learning framework for predicting cyber attacks rates*. Accessed on 28 Oct 2017. URL: https://sci-hub.do/https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-019-0090-6.