

# RESEARCH PROPOSAL PRESENTATION

Bridging the human weakness gap: How to use Predictive Analytics  
and Machine Learning technology to detect patterns in human  
behaviour and predict cyber-attacks?

University of Essex Online (UoEO)  
Research Methods and Professional Practice (RMPP)

Student: Mohamed Danialou

Student ID: 12688774



# INTRODUCTION

## Background

- Predictive Analytics, Machine Learning & Artificial Intelligence have revolutionized the way we use data to predict the future (Janiesch et al., 2021; Haenlein & Kaplan, 2019; Mikalef et al., 2018).

## Issues

- Predictive Analytics is based on anomaly detection which is prone to high rates of False Positives (MIT, N.D.).
- Human is the weakest link in the cybersecurity chain (Hadlington, 2017).

## Consequences

- Loss of Confidence and trust (MIT, N.D.).
- Humans' behaviour did not change to positively affect the trend in attack reduction (Maalem et al., 2020).



The detection and prediction of patterns of human behavior have been the subject of much research. The huge leaps in the technology field with the development of cutting-edge technologies such as Machine Learning (Janiesch et al., 2021), Artificial Intelligence (Haenlein & Kaplan, 2019), and Big Data Analytics (Mikalef et al., 2018) have revolutionized the way organizations use data to predict the future and identify patterns that may be responsible for certain events that impact their operations, especially the protection of their most critical assets.

Although Predictive Analytics, Machine Learning, and Artificial Intelligence (individually) have provided new ways to predict and detect threats, they have somehow failed to significantly reduce cyber-attacks and close the security gap due to being based on anomaly detections which are prone to high rates of false positives that create doubt in the system and therefore affects confidence and expectation (MIT, N.D.).

As the weakest link in the cybersecurity chain (Hadlington, 2017), humans are a consistent yet unpredictable presence that is inherently vulnerable and prone to behaviour that may jeopardize the security of organizations and their assets. Studies on human factors and their consequences on cybersecurity have not changed humans' behavior to positively affect the trend in attack reduction (Maalem et al., 2020). As powerful and advanced as machines are, the presence of a user is sufficient to defeat the most powerful technology. This is shown by the increasing number of attacks that occur as a result of human errors (Maalem et al., 2020).

However, there is a lack of research on how this issue can be resolved and enhance the technology to improve the prediction rate to detect cyber-attacks, especially with the acceleration of the digitization of our lives as a result of the Covid 19 pandemic and the prevalence of the Internet of things (IoT). Therefore, it is necessary to take a different approach and find a better and improved method to predict patterns that are consistent with negative cybersecurity behaviors.

The combination of Predictive Analytics with Machine Learning and input from human experts could provide a better and more effective way to predict patterns of human behaviour and get better results by reducing the rate of false positives and the need for continuous fine-tuning.

Predictive Analytics can help organizations identify risks and predict trends or behavior based on big data (Kumar & L., 2018).



## SIGNIFICANCE - CONTRIBUTION TO THE DISCIPLINE - RESEARCH PROBLEM.



➤ Data feeds



➤ Feedback



➤ Confirmation



Predictive Analytics is a technology that uses data to predict the future. It relies on present and historical data to predict behaviour and find the unknowns. It works with Big Data Analytics which is another technology that is used to collect and centrally store data from users, systems, and applications in a data lake where the data is then subject to all sorts of analyses and processing. Predictive Analytics can help organizations identify risks and predict trends or behavior based on big data (Kumar & L., 2018).

The implementation of Predictive Analytics is not a simple process as it requires a number of steps that must be meticulously implemented to yield good results.

**Requirements:** It is the first step of the development process as it enables requirements such as scenarios and use cases to be collected. This information will be used to predict the patterns during the development of the predictive model. The main question here is to determine what is to be achieved for the development of the predictive model.

**Data collection:** This is the process of collecting and centralizing the storage of data generated from multiple sources such as users, systems, applications, etc. to enable the analysis and processing. This process requires the implementation of a big data analytics platform or tool to convert unstructured datasets to structured data ready for processing. There are various proprietary and open-source technologies such as Apache Spark (Apache, 2019), Hadoop (Apache, 2019), Cassandra (Apache, N.D.), and Splunk (Splunk, N.D.), etc. that can be used for this task.

**Data analysis and processing:** In this step, the stored data is formatted, and converted to a structured form for ease of processing. It is tested for its quality and for the presence of errors.

**Machine Learning:** This step requires a machine learning model to be developed using one of the following techniques.

- Artificial Neural Networks: They are another form of Machine Learning in which a computer learns to perform some tasks by being fed artifacts similar to a human brain that is being trained to perform certain tasks (Hardesty, 2017).
- Decision trees: They are decision-making processes represented in graphs and their outcomes from qualitative and quantitative perspectives (Tewari et al., 2017).
- Support vector machines: They are sets of machine learning methods that focus on classification, regression, and outliers detection. (Meyer, 2015)

These models are applied to the data to detect patterns hidden in data streams.

**Predictive Modeling:** In this step, a predictive model is developed based on the selected machine learning technique and the collected structured data. The model is tested on the data and the result is analyzed for errors.

**Prediction monitoring:** The predictive model is deployed, and results and reports are generated and analyzed. The model is also analyzed for false positives and fine-tuned as required.

The above-listed steps are the steps used to implement predictive Analytics solutions. However, although this method is effective in creating a good solution, it does not always guarantee the right results and is prone to high rates of false positives and it requires continuous fine-tuning, which impacts the quality of predictions and the rate of true positives.


The limitation here is that the effectiveness of the prediction depends largely on how big the dataset is, and the scenarios fed to it. The other issue is that the predictions are based on anomalies that require constant fine-tuning and testing.

Many organizations today have predictive analytics solutions deployed in their environments or as a cloud solution. However, they still face constant attacks, some of which are successful and not predicted by the solution.

This study aims to propose two additional steps and methods to enhance the prediction rate of the solution by adding the following steps:

- Data feeds: Real-life cyber-attack scenarios and threat intelligence data from expert analysts will be fed to the model to enable predictions to be more accurate and reduce the rate of false positives.
- Feedback and confirmation: The solution will be enabled to constantly provide feedback to the expert analysts which will then be analyzed, and the results confirmed or adjusted accordingly.

The expectation by including these additional steps is for the predictions to be more accurate, and the rate of false positives to decrease.



## RESEARCH QUESTION & OBJECTIVE



➤ False Positive Rates.



➤ Missed Behaviour



➤ New Patterns



➤ Quality



The current predictive analytics solution detections have not positively translated to a significant reduction in cyber-attacks as a result of human errors. The rate of false positives and missed behaviours have hampered the efficacy of the solution and increased distrust and loss of confidence.



The objective of this research is the following:

1. To add a layer of validation with input and feedback to the predictive solution to make it more effective.
2. To reduce the rate of false positives by ensuring the new input and feedback add value to the solution.
3. To reduce the rate of missed patterns and increase the rate of detected patterns.
4. To increase the rate of predicted behaviour.
5. To significantly increase the rate of predicted cyber-attacks.

The research aims to explore the following questions and find answers that could be used to understand how the new method has enhanced the detection mechanism of patterns and prediction of behaviour.

In order to answer these questions, there will be a benchmark of the existing predictive solution prediction rates of false positives, missed behaviour, and attacks.

1. How do the results in terms of the percentage of false positives and missed behaviours of the new method compare with the percentage of these artifacts in the old method?
2. How did the new method affect the detection of patterns and the percentage of artifacts (false positives and missed behaviour)?
3. What is the percentage of new patterns detected?
4. What are the differences in terms of the quality of patterns detected compared to the old method in how the machine learning model processes new inputs and expert feedback?



**KEY LITERATURE**

- Identification and Prediction of Human Behavior through Mining of Unstructured Textual Data (Davahli et al., 2020).
- Analysis of Human Behavior by Mining Textual Data (Gutierrez et al., 2021).
- Creative Persuasion (Rajivan & Gonzalez 2018).
- Statistical Models for Predicting Threat Detection From Human Behavior (Kelley et al., 2018).
- Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning (Yeboah-Ofori & Boachie, 2019).

The following literature will be used as part of the research.

- Identification and Prediction of Human Behavior through Mining of Unstructured Textual Data (Davahli et al., 2020).
- Analysis of Human Behavior by Mining Textual Data: Current Research Topics and Analytical Techniques (Gutierrez et al., 2021)
- Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks (Rajivan & Gonzalez 2018).
- Statistical Models for Predicting Threat Detection From Human Behavior (Kelley et al., 2018)
- Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning (Yeboah-Ofori & Boachie, 2019)



The research will be conducted using existing literature and information collected from multiple reliable academic sources such as Google Scholar, Research Gate, University of Essex Online (UoEO) library, Springer, Jstor, ScienceDirect, and other online libraries to better understand the working process of the predictive solution, the difficulties in reducing the rate of false positives and the reasons the solution is failing to meet organizations' high expectation.

The research will also look at use cases and examples of existing implementations available in the public domain to better understand the solutions' limitations and issues.

To be able to enhance the solution with real-life attack scenarios and threat intelligence feeds, a number of expert analysts with experience in cybersecurity will be approached through a survey to participate in the proof of concept. The survey will have a questionnaire with open-ended and close-ended questions, demographics of participants, their seniority in terms of the number of years of experience in cybersecurity, their area of expertise such as Data Science adapted to cybersecurity, Blue team, Red team, or Purple team, Governance, Risk & Compliance (GRC), etc.

Access to the predictive analytics solution will be given to the participants to enable them to ingest their scenarios and attack simulation feeds with feedback sent automatically to each participant after their scenarios have been processed.

Additionally, subscriptions will also be made to open-source threat intelligence feeds such as Google Virus Total and Mandiant, etc. to collect artifacts such as Tactics, Techniques, and Procedures (TTP), Indicators of Compromise (IoC), and Behaviour of Compromise (BoC).

## ETHICAL CONSIDERATIONS AND RISK ASSESSMENT



Consent

➤ Consent



➤ Anonymisation



➤ References




Participants who are taking part in this research will need to provide their explicit consent. The consent form will provide details of the study, the objective, goal, scope, what collected data will be used for, etc. The form will also ensure participants know that their involvement is voluntary and that they could withdraw at any stage of the study.


In order to ensure a fair and unbiased study and feedback, collected personal identifiable information (PII) will be anonymised or randomised.

Additionally, all literature materials used as part of this study will be cited and referenced as per the University of Essex Online (UoEO) Harvard Referencing Guide.

The result of the study will be peer-reviewed before it is released to ensure the study process met all requirements and guidelines and data manipulation did not occur during the process. Once the review has been finalised and concurred, the result will be released and shared with participants and other parties interested in such studies.

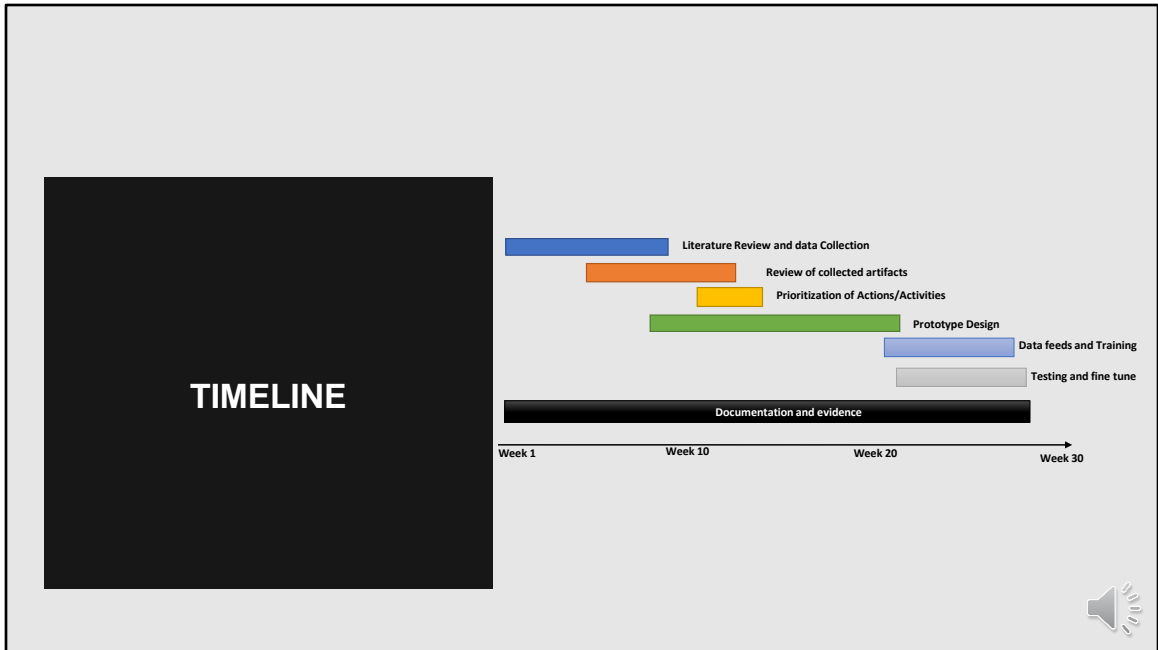


**ARTIFACTS TO BE CREATED**

-  ➤ Predictive Analytics
-  ➤ Big Data Analytics
-  ➤ Evidence

The predictive analytics with machine learning capability prototype will be developed. And if possible big data analytics will be deployed as well.





The timeline for the proposed activities is 30 weeks and will be as follows:

1. Research: Literature and data collection 5 weeks
2. Review of collected artifacts: 5 weeks
3. Prioritisation of actions: 1 week
4. Design of predictive analytics solution: 10 weeks
5. Data feeds and training: 3 weeks
6. Test and fine-tuning: 3 weeks
7. Documentation and evidence: 3 weeks

## References

- Apache Cassandra (N.D.) Apache Cassandra Documentation. [online] Available at: [https://cassandra.apache.org/\\_/index.html](https://cassandra.apache.org/_/index.html) [Accessed 16 Nov. 2022].
- Apache Hadoop (2019). Apache Hadoop. [online] Available at: <https://hadoop.apache.org/> [Accessed 16 Nov. 2022].
- Apache Spark (2019). Apache Spark™ - Unified Analytics Engine for Big Data. [online] Available at: <https://spark.apache.org/> [Accessed 16 Nov. 2022].
- Davahli, Mohammad Reza et al., (2020). Identification and Prediction of Human Behavior through Mining of Unstructured Textual Data. *Symmetry*, 12. 10.3390/sym12111902.
- Gutierrez, E., Karwowski, W., Fiok, K., Davahli, M.R., Uciaga, T. and Ahram, T. (2021). Analysis of Human Behavior by Mining Textual Data: Current Research Topics and Analytical Techniques. *Symmetry*, 13(7), p.1276. doi:10.3390/sym13071276.
- Hadlington Lee (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3 (2017) e00346. doi: 10.1016/j.heliyon.2017.e00346 <http://dx.doi.org/10.1016/j.heliyon.2017.e00346> 2405-8440
- Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61(4), 5–14. <https://doi.org/10.1177/0008125619864925>
- Hardesty, L. (2017). Explained: Neural networks. [online] MIT News. Available at: <https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414> [Accessed 17 Nov. 2022].
- Janiesch, C., Zschech, P. & Heinrich, K. (2021) Machine learning and deep learning. *Electron Markets* 31, 685–695 <https://doi.org/10.1007/s12525-021-00475-2>
- Kelley T, Amon MJ and Bertenthal BI (2018) Statistical Models for Predicting Threat Detection From Human Behavior. *Front. Psychol.* 9:466. doi: 10.3389/fpsyg.2018.00466
- Maalem Lahcen et al., Review and insight on the behavioral aspects of cybersecurity. *Cybersecur* 3, 10 (2020). <https://doi.org/10.1186/s42400-020-00050-w>
- Massachusetts Institute of Technology. (N.D.). System predicts 85 percent of cyber-attacks using input from human experts. [online] Available at: <https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418> [Accessed 17 Nov. 2022].
- Meyer, D. (2015) Support Vector Machines. The Interface to libsvm in package e1071. [online] Available at: <https://mran.revolutionanalytics.com/snapshot/2016-03-14/web/packages/e1071/vignettes/svmdoc.pdf> [Accessed 17 Nov. 2022].
- Mikalef et al., (2018) Big data analytics capabilities: a systematic literature review and research agenda. *Inf Syst E-Bus Manage* 16, 547–578 (2018). <https://doi.org/10.1007/s10257-017-0362-y>
- Rajivan P and Gonzalez C (2018) Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Front. Psychol.* 9:135. doi:10.3389/fpsyg.2018.00135
- Splunk. (N.D.). Data Optimization. [online] Available at: [https://www.splunk.com/en\\_us/solutions/data-optimization.html](https://www.splunk.com/en_us/solutions/data-optimization.html) [Accessed 16 Nov. 2022].
- Tewari, Puran & Mittal, Kapil & Khanduja, Dinesh. (2017). An Insight into "Decision Tree Analysis". *World Wide Journal of Multidisciplinary Research and Development*. 3. 111-115.
- Vaibhav Kumar & L., M. (2018). Predictive Analytics: A Review of Trends and Techniques. *International Journal of Computer Applications*. 182. 31-37. 10.5120/ijca2018917434.
- Yeboah-Ofori A. and C. Boachie (2019), "Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning," *International Conference on Cyber Security and Internet of Things (ICSIoT)*, 2019 , pp. 66-73, doi: 10.1109/ICSIoT47925.2019.00019.

