***Acknowledgments***

In the Name of ***ALLAH,*** the Most Gracious and the Most Merciful.

We thank God for helping us accomplish this modest work.

We would like to take this opportunity to express our deepest thanks and gratitude to our supervisors: Mr. Mokaddem and Mme. Mokhtari for their availability, advice, guidance, and their encouragement throughout our research.

We would like to express our sincere gratitude to the members of the jury who agreed to evaluate and examine this work, particularly to:

Finally, our warmest thanks to everyone who has participated in any way in the success of this modest work.

**Summary**

The world has never been more connected than it is today. The Internet has become critical to our everyday lives, businesses, individual needs, and so has its security. With our growing dependence on networked digital systems comes an increase in the variety and scale of threats and cyber-attacks.

Cybersecurity is an important aspect of any system or application’s life, ranging from basic personal privacy and well-being to outright important and sensitive international data. Big tech companies are held to high standards when it comes to the safety of their customers’ information, thus, they cooperate to achieve greater levels of security.

This field requires speed and an immense amount of variant data to produce reliable and performant anti-infiltration systems. That is the reason why companies have shifted from the traditional relational model in this domain to trying to adopt new suitable solutions and methods, with some of those methods being in the operational stage and others in the study stage. For our project, we will be focusing on one of the solutions at the study stage which is the introduction of knowledge graphs to cyber security for improving the accuracy of attack detections.

Knowledge graphs have shown great potential in cyber security because of their capabilities in knowledge management, aggregation, representation, and reasoning.

Therefore, the main objective of this project is to set up a commonly used NoSQL database store that would contain the NSL-KDD dataset in the form of RDF, which would later be used to construct knowledge graphs in order to find patterns, identify and track attack paths, and filter out intrusions from normal connections as a way of detecting attacks.

***KEYWORDS:* Cyber security, NoSQL, RDF, intrusion detection systems, NSL-KDD, Datacenter, Knowledge graphs.**

SOME info I found interesting:

It provides a novel feature for improving the accuracy of cyber security situation detection by abstracting the attack events (e.g., historical events, Internet news) as graph description

In cybersecurity, a graph-based approach centers on preserving the context of security events by breaking down components of observable data into a graph representation of all cyber artifacts, from all data streams, accounting for all past and present data.

A knowledge graph creates a digital twin of your environment, enabling you to represent all or part of your network data in a holistic view. This view is very useful for cybersecurity analysts to query and take action on. In addition, the knowledge graph can be analyzed by data scientists, who build models to detect malicious activities.

Your graph may include events like:

* + User access events
  + Application resources usage
  + Devices connected
  + Service health

NIST, and others have created vulnerability databases that are used industry-wide. By ingesting this data into your graph, you can see where the vulnerabilities impact critical resources and reveal potential attack paths to those resources.

Attack paths take the attackers’ perspective and show the path of potential multistage attacks along with the vulnerabilities used at each stage. This process goes beyond a static list of vulnerabilities and looks at how an attacker could use them.

An attack path analysis can identify different paths an attacker may take through your infrastructure to reach those assets. All the attack paths on a network together form an attack graph. Visualizing the paths as a graph is intuitive, especially with a graph data visualization tool such as Neo4j Bloom.