2.1 Introduction

A review and synopsis of the body of work on this project are given in this chapter. The project's terminology will be discussed, and some relevant publications will be reviewed. The topics of conversation included Deep Machine Learning, Intrusion Prevention Systems, And Intrusion Detection Systems.

2.2 Overview of Intrusion Prevention System

2.2.1 Definition of Intrusion Prevention System

According to (Nick Ierace, Cesar Urrutia, and Richard Bassett, 2019), Intrusion Prevention System is an advanced version of Intrusion Detection System. Intrusion Prevention System (IPS) is devices that no matter hardware or software that has the ability to detect both well-known or unknown attacks, and also prevent the attack from being successful.

2.3 Review of Related Works

2.4 Related Techniques and Methodology

2.5 Conclusion

As a conclusion, web-based Intrusion Prevention System is more way effectives than software type

\*\* Singh, A.P. (2020) stated that an Intrusion Detection System (IDS) is an application device or software that controls and monitors network or system activities to ensure that no malicious tasks are being carried out. IDS detects and checks for any unwanted activities and plays a crucial role in improving network security and protecting organizational data and information. \*\*

# References

Nick Ierace, Cesar Urrutia, and Richard Bassett. (2019). Intrusion Prevention Systems. *ACM Ubiquity*.

Singh, A. P. (July, 2020). Intrusion Detection System. *International Journal of Engineering and Techniques*, 9.