# **INTRODUCTION**

Information security is a significant aspect of communication, which involves safeguarding data and information from unauthorized access and tampering. The protection of sensitive information ensures that it remains confidential and that it cannot be altered by unauthorized users. The secure transmission of data from one entity to another is crucial, and the rise in the number of information attacks over the last few decades highlights the importance of implementing effective information security measures [1]. Cybercriminals attempt to capture valuable information for their own purposes. The security of an organization's information depends on various types of data that the organization possesses.

As the world increasingly becomes connected through the internet, it has become necessary for businesses to migrate onto the internet. This has increase the number of buying and selling on the internet. The introduction of covid-19 led to an increase in online transactions due to the fact that countries all over the world went into quarantine. This made businesses and jobs operate remotely through the internet, therefore, there was a drastic increase in the number of phishing attacks on organizations and individuals [2].

# **REFERENCES**

1. Li, M., Nazir, S., Khan, H. U., Shahzad, S., & Amin, R. (2020). Modelling features-based birthmarks for security of end-to-end communication system. *Security and Communication Networks*, *2020*, 1-9.
2. Subasi, A., Molah, E., Almkallawi, F., & Chaudhery, T. J. (2017, November). Intelligent phishing website detection using random forest classifier. In 2017 International conference on electrical and computing technologies and applications (ICECTA) (pp. 1-5). IEEE.
3. Muppavarapu, V., Rajendran, A., & Vasudevan, S. K. (2018). Phishing detection using RDF and random forests. Int. Arab J. Inf. Technol., 15(5), 817-824.