Literature Survey

- **Workman** conducted a theory grounded investigation on social engineering threats by applying hypothesis on user behaviour. The user behaviour was evaluated based on six hypotheses that are derived by utilising the concept of commitment, reciprocation, consistency, social proof, likeability, trust, fear, authority, and scarcity. From the study, it is found that high normative commitment, high continuance commitment, and high affective commitment are more important in successful social engineering attacks. Yet this work fails to investigate relationships among personal factors and social engineering outcomes. This study only involves hypothesis testing instead of a demographic model building.
- **Wang et al** conducted an investigation to acknowledge the impact of phishing attack by sending a real spear-phishing email to targeted victims. From this survey, it is inferred that attention to visceral triggers, attention to phishing deception indicators and phishing knowledge has a huge impact on phishing detection. Anyhow this study explores only spear-phishing attacks and relies on cognitive-effort measure and one-round survey.
- **Alsharnouby et al** conducted an empirical study against phishing attacks by allowing users to access the browser security indicators to create awareness among them. Major web browsers used for this experiment are Microsoft Internet Explorer 10, Mozilla Firefox Version 10.0.12, Google Chrome Version 26.0.1410.43, and Apple Safari Version 6.0.3. At the end of the experiment, it is found that even in a controlled environment, participants had an average success rate of 53% for identifying phishing websites, which is equivalent to the random guess.
- **Khonji et al** presented a survey on overview of phishing mitigation techniques. However, this survey does not cover all the notable evaluation metrics that are language independency, third party independence, and zero-hour attack detection while evaluating the existing detection approaches.
- **Varshney et al** presented a survey on web phishing detection schemes. This paper surveyed about various existing anti-phishing solutions, such as blacklists and whitelists, domain name system (DNS)-based phishing detection, proactive phishing uniform resource locator (URL)-based phishing detection, heuristics and machine learning (ML), and search engine-based detection. Unlike Khonji et al. [21], this work focuses on the detection technique alone and discusses the evaluation metrics such as language independency, third party independence, and zero-hour attack detection. Search engine-based detection techniques are considered as a better solution in that survey but they tend to provide high false-positive rate (FPR) on webpages with zero-day life span. This survey does not cover the hybrid approaches of web phishing detection techniques.
- **Tewari et al** presented a survey on various defence mechanisms against phishing attacks. This paper simply provides a survey of current web anti-phishing solutions and fails to cover all the detection mechanisms available to mitigate the attack.
- **Jain and Gupta** surveyed visual similarity-based web antiphishing solutions and presented their comparative study. It is inferred from the survey that most of the approaches still have boundaries against accuracy, new phishing websites, detecting embedding objects, and so forth. However, this survey focuses on visual similarity-based web phishing detection only.
- **Dou et al** presented a survey on the systematic study of phishing detection schemes. The taxonomy presented in this paper does not include the deep learning methodologies and

simple evaluation metrics such as accuracy, true positive rate (TPR), and FPR are applied to assess the performance of detection approaches.

- **Goel and Jain** presented a survey about the mobile phishing attack and its life cycle. This study also surveyed the various technical approaches includes mobile malware, wireless medium, content injection, and online social networks, and technical subterfuge that the attackers used to compromise the security of the mobile phones in the smartphone environment. However, this paper mainly focuses on the mobile phishing attack and its technical approaches only.
- **Chiew et al** surveyed about the phishing techniques deployed in the detected phishing attacks so far. This paper also reviewed the characteristics of the medium and the various vectors of phishing. This paper fails to study detection mechanisms.
- **Qabajeh et al** conducted a review on the phishing detection approaches using ML algorithms especially associative classification and rule induction and failed to cover all other detection techniques. Even though numerous surveys are existing in the literature, there is no work to the best of our knowledge which explains in detail all the existing web phishing detection techniques. The majority of the existing survey provides only a concept-oriented description whereas this paper aims to present all the state-of-theart web phishing detection techniques and attempts to evaluate every technique with the standard set evaluation metrics.