Abstract
In consideration with the security of user on the Internet, Phishing remains an important threat. Currently working systems are based on reactive URL blacklisting technique which is inefficient due to short lifetime of Phishing websites and unavailability of newly launched Phishing sites. In the proposed system we introduce a real-time automated phishing detection system for e-mails which can analyze an URL present in the context of an e-mail to identify potential Phishing sites. Along with the URL, contents of emails are also checked with intra-URL relatedness. Phishing URL’s have relationships between their first part (lower domain) and remaining part (upper domain) like path, file folder, etc. URL uniqueness is figured out by evaluating it using identical properties extracted from keywords that compose a URL based on the query data from Google and Yahoo search engines.

References

- Yanhui Du, Fu Xue "Research of the Anti-Phishing Technology based on E-mail extraction and analysis."
- Samuel Marchal, Jérôme François, Radu State, and Thomas Engel "PhishStorm: Detecting With Streaming Analytics"

Index Terms

Computer Science
Information Sciences
Keywords
Intra-url Relatedness  Mails  Phishing Detection  Lower Domain  Upper Domain.