Instant Messengers play a key role in binding the people all over the world through the internet at not only the personal but also at the e-commerce level. The IMs possess the state of the art features like exchanging free instant messages, voice chatting, video chatting, file sharing, maintaining buddy lists etc. User ignorance towards the use of communication services like IMs, emails, websites, social networks etc. is becoming the biggest advantage for phishers. As there does not exist, any permanent solution to the phishing problems, efforts could be made in the direction to minimize the impact of phishing. The possible solution to this issue is firstly to create technical awareness in users by educating them and secondly to create a phishing detection application which would generate phishing alerts for the user so that phishing messages are not ignored. For reliable, secure and trust worthy Instant messaging services, efforts have been made on a regular basis to improve its efficiency and performance. The lack of basic security features to detect and prevent phishing has had a profound effect on the IM clients, as they lose their faith in e-banking and e-commerce transactions, which will have a disastrous impact on the corporate and banking sectors and businesses which rely heavily on the internet.

Various solutions to phishing detection and prevention exist in websites, URLs, emails and social networking systems, even anti-
phishing plug-ins have been developed for detecting fake websites. But, very little research contributions were available in for phishing detection in Instant messengers.

The phishing detection in the past used pre-defined blacklisted phishing words were used for matching and could not detect the zero-hour phishing attacks. To overcome the blacklisting problem, phishing heuristics i.e. experience based methods of problem solving were also used. Various data mining techniques like association rule mining (ARM), classification and clustering have also been used to detect phishing dynamically, but the approaches were all content based and there was no considerable decline in the false positives and the false negatives.

A context based, dynamic and intelligent phishing detection methodology in IMs is proposed, to analyze and detect phishing in Instant Messages with relevance to domain ontology and utilizes the Classification based on Association (CBA) for generating phishing rules and alerting the victims.

This system utilizes the proposed PDS Monitoring system algorithm in identifying the phishing activity during exchange of messages in IMs, with high ratio of precision and recall. It contains two main components: Ontology Based Information Extraction (OBIE) and Classification Based on Association (CBA).
In the OBIE, the Instant messages exchanged are preprocessed by removing the stop words and performing the stemming operation to generate filtered keywords. These keywords are mapped for their relevant domains and context from the ontology inference engine using the modified Triplet algorithms. In case of discovery of new domains, they are appended to the domain ontology along with their semantic lexicons and instances. The obtained attribute values of the domain ontology and context along with the threshold values serve as the testing dataset for the generation of Classification Association Rules (CAR).

Pre-defined phishing rules serve as the Training dataset for Associative classification, which have been framed by experts from the phishing domain with extensive experience. The Classification based Association (CBA) is applied to the test data to predict the phishing words which are classified as Phishing, Suspicious or Normal words through colour indicators for alerting the victim client.

The context based phishing detection in Instant messengers has been demonstrated empirically using 110 chatting transactions and implemented through the PDS monitoring system. The results have shown improvement by the increased percentage of precision and recall when compared to the existing methods. A comparative analysis with the existing solutions demonstrates the better performance of the presented work.
An overall effort has been made through this research work and its implementation, to re-instate the lost trust and apprehensions the users had in using the online banking and commercial applications and to use them with more technical awareness and confidence to overcome their own vulnerabilities from being deceived by the phishers at large.