CHAPTER 1

INTRODUCTION

1.1. OVERVIEW OF THE RESEARCH WORK

Opinions contour the central point of all human activities and are the prominent influencing factor of day-to-day actions (Petr *et al.*, 2020). From olden times, people's normal tendency is to consider information gained from other people's opinions important while deciding on things. For example, people often try to find answers to questions like,

- Which product works better and which one can I buy?
- Which hospital/doctor provides the best treatment?
- Which school/college suits my ambitions regarding a specific subject?
- Which restaurant has good, tasty, economical and healthy food?

In the pre-Internet era, this kind of information was obtained from friends, books, newspapers, relatives, etc. In the post-internet era, such information is available in the form of online reviews and is being used frequently by users.

The development of e-commerce sites along with the wide usage of World Wide Web (WWW) has attracted millions of people worldwide to shop online. According to Law (2021), more than 2.14 billion globally buy products and services online and account for 18.1% of retail sales worldwide. Moreover, it is expected to increase tremendously in near future. It was noted by Chadchankar *et al.* (2020), a majority of persons (81%) conduct online research about the product they wish to buy, before actual purchase and if they find that verified buyers have experienced poor customer service, then more than 58% of online purchasers stop doing business with them. This shows that opinions or reviews on products sold, presented as feedbacks of buyers, are most trusted by buyers and have a huge influence during a purchase (Zhang *et al.*, 2020b).

The online reviews can be obtained from numerous sources, which has raised one important question –"How far the information provided by online reviews are genuine?". But, oftentimes, reviews are used to provide untrue facts which break the guidelines of the

business and undermine the integrity of the e-commerce site on which it appears. These reviews called spam reviews or fake reviews or bogus reviews or deceptive reviews, are defined as the usage of illegitimate and intemperate methods for generating jillions of fake reviews for provoking unfairness positive or negative opinions, with the intent of either promoting or demoting a target product or service (Hajek *et al.*, 2020).To safeguard naïve users from being vulnerable to unethical acts, e-businesses must detect and remove phoney reviews.

The solution to this is the use of an Online Spam Review Detection (OSRD) System. The OSRD system's principal purpose is to identify authentic, honest (ham) reviews and remove fake (spam) reviews (Sonia, 2020).Both internet users and online organizations dream of a system that can differentiate ham and spam reviews in an accurate and fast manner. Currently, there are too many sources that can be used to write reviews and as a consequence, the number of available reviews has also increased. This has resulted in too much information, with too few tools to process them. Thus, regardless of numerous solutions proposed to achieve this goal, this fantasy is as yet not yet a reality, and exploration in this field is still dynamic.

To turn down the divergence between this reality and dream, this research work proposes algorithms that enhance each step of ORSD, which when cumulatively used can produce an efficient system with high detection accuracy. This study presents strategies for detecting review spam by taking into account spamming features associated with reviews, reviewers, and products. The work also exploits data mining algorithms, in particular, the usage of classification and clustering-based machine learning algorithms. Hybrid systems combining clustering and classification algorithms are proposed.

The proposed spam online review detection is a part of the security aspect of online review, as it protects users (or buyers) from fake details. The proposed system extensively uses opinion mining, a sub-field of data mining, for identifying fake reviews for e-commerce applications. In particular, the proposed system uses feature engineering, classification, and clustering algorithms to improve online spam detection. This section gives the introductory materials identified with the research subject along with the formulated research objectives.

1.2. ONLINE REVIEWS

Generally, customers learn about a product and its quality through advertisements and review websites. However, the WWW has made it easier for people to share their views and opinions on the products sold by e-commerce websites. The WWW supports direct communication between the sellers and buyers and also allows both of them to obtain information in the form of reviews, which are posted in several applications like social media networks (Example : Twitter, LinkedIn, Facebook), E-commerce websites/online commercial shops (Example : Amazon, eBay, Flipkart) and Blogs (Luo *et al.*, 2013). Apart from these applications, several review websites like Yelp, TripAdvisor, also exist. These allow individuals to post reviews on a wide variety of topics like businesses, famous personalities, products and services.

Upsurge in the number of e-commerce websites is attracting a large number of users to purchase products and services online(Wadhawan and Arya, 2020). The e-commerce websites, allow the customers to post their opinion or comments on their purchasing experience and level of satisfaction regarding the goods bought or services utilized**.** These opinions are shared by the e-commerce websites in the form of online reviews and which are accessible to both other customers and the business itself.

The level of satisfaction regarding product quality is often provided through a combination of a1-5 star rating scale, like / dislike and reviews (Chen, 2013). The rating scale allows reviewers to grade the quality of their purchase, where a 1-star rating indicates poor quality and a 5-star rating indicates the apical quality. According to Luca (2016), business revenue can be positively affected by 5-9%, even with a 1-star negative rating. A similar opinion was also provided by Marchang (2017), who said that even a single negative review can create a colossal impact on businesses and often results in losing approximately 22% of customers. Conversely, too many positive reviews also may bring down the business, as users may assume that all are fake. Thus, online reviews often work as testimonials and are used almost by all internet buyers.

An online review is defined as a positive, neutral or negative statement, which is created by a former consumer, about a commodity or a company and made available to the public through the Internet (Chen *et al.*, 2018). Analogous to this, Liu (2012) has also

defined opinions or Reviews are essentially an opinion holder's favourable or negative mood, view, attitude, emotion, or appraisal of an entity or a part of the entity. Here entity refers to a product, a popular personality, a social event, a service provided, an issue or a company. Another popular definition of review is given by Rastogi *et al.*, 2020 and is described below.

A user review 'r' is a review for a product or service written by a user or consumer based on their experience as a user of the reviewed product. The following information is frequently included in a review:

- A brief passage of text or note conveying the user's impressions and opinions about the evaluated product.
- The reviewer's rating of the product. It's anywhere between a predetermined lowest and greatest value, commonly in the [1,10] or [1,5] range.
- The review's creation date and time.
- The review's author, either known or anonymous.

1.2.1. Advantages of Online Reviews

The online reviews consist of raw information regarding the activities of the website and if handled efficiently, can provide valuable information to both individuals and the organization (Absaitovna and Jamshedovna, 2020). For potential customers, the posted reviews provide details that help them to narrow down the various options available and help them to make sound decisions based on their needs and quality. In other words, they can be used to make the right decision on selecting a product they wish to buy. Buyers use them before purchase, as they are fast and provide up-to-date information regarding the product to be purchased in an easy-to-understand format (Schuckert *et al.*, 2015). Moreover, as online reviews are considered as electronic word-of-mouth (eWOM) version, it is used by maximum buyers (Lee and Lee, 2009).

On the other hand, the e-commerce companies consider reviews as 'the wisdom of the crowd' and use them to obtain knowledge that can be integrated with strategies to attract customers and improve sales (Dai *et al.*, 2019). Business holders and manufacturers can gain knowledge on customer needs, identify weaknesses in their product(s) and/or

services(s), develop methods to increase customer retention and improve customer satisfaction, implement methods to increase sales and finally, help to understand competitor's condition in the market and strategize methods to improve their business state towards success. Thus, online reviews have tremendous usage on both individuals and businesses. However, the benefits, so far, spoken of its possible only when the information source (the review) being truthful. The uprise in number of online e-commerce sites has also increased the applications that gather their experience of customers through questionnaires or reviews.

1.2.2. Types of Online Reviews

Online reviews are considered important to a business because they act as social proof, which provides several advantages like increased purchases, more online visibility and generate more traffic to the business. The three main components of an online review analysis system are the user, the object and polarity orientation (Liu and Karahanna, 2017). Here, the first component refers to the person who writes or reads the review and may denote either the consumer or the spammer. The second component object is the product for which the opinion is written and the third factor decides how an opinion is positive, negative or neutral.

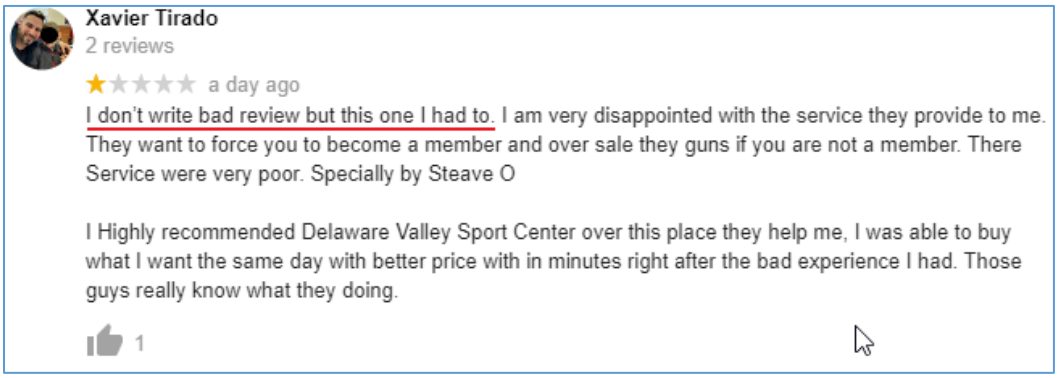
Positive reviews hold superlative text and/or have a higher rating scale (4-5 stars). On the other hand, negative reviews have text with words that degrade the product and/or have very low ratings (1-2 stars) (Fullerton, 2017). Examples of positive and negative reviews are given in Figures 1.1 and 1.2 respectively.

The positive and negative reviews can further be grouped into three types, as given below (Dixit and Agrawal, 2016)

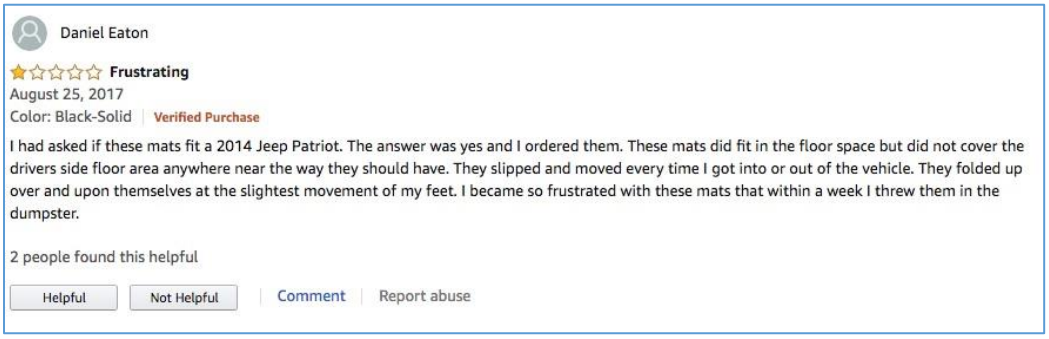
- Type 1 (Fake/Untruthful/Bogus Reviews)

  These are written with hidden motivations rather than based on the reviewers' true experiences. They're utilised to smear the internet review system's credibility.
  These are written not based on the reviewers' genuine experiences but are written with hidden motives. They are used to undermine the integrity of the online review system. They often contain

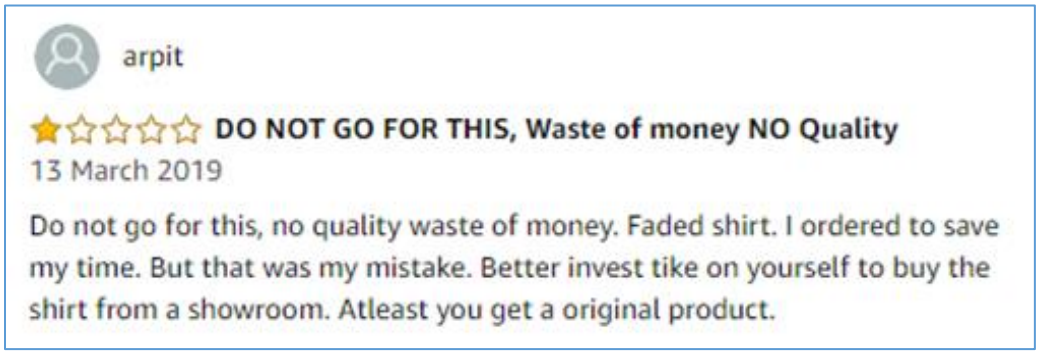
- They frequently feature unjustified positive judgments about certain target entities (products or services) in order to promote the entities→Hyperspam.
- Spreading unjust or misleading negative thoughts about others in order to harm their reputations→Defaming spam.



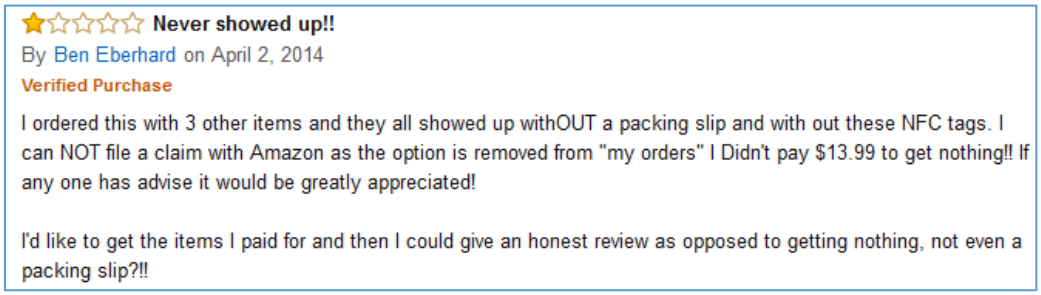
(a)



(b)

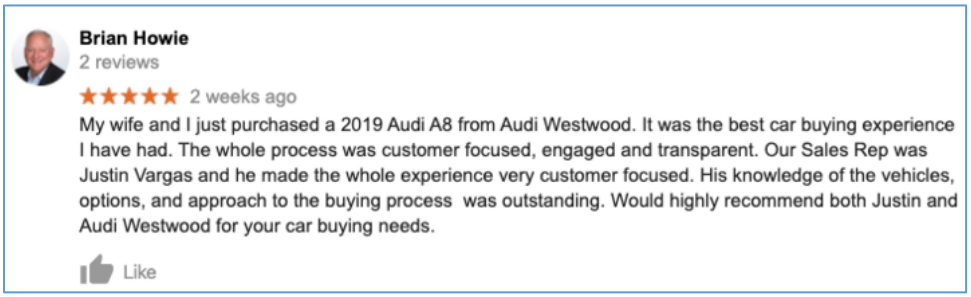


(c)

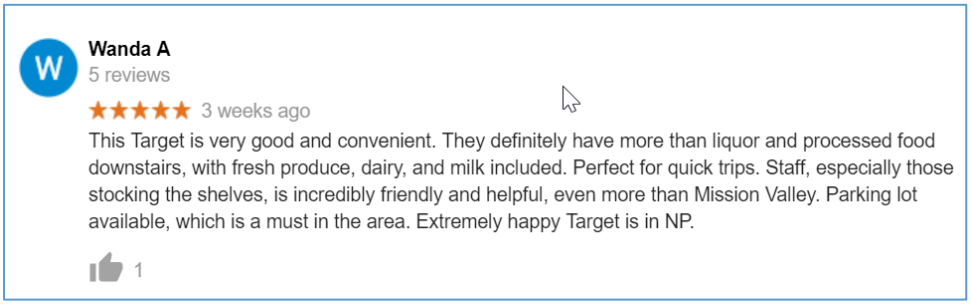


(d)

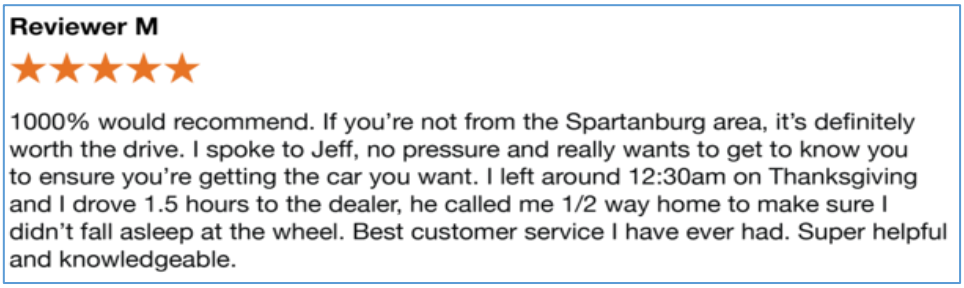
Figure 1.1 : Examples of Negative Online Reviews



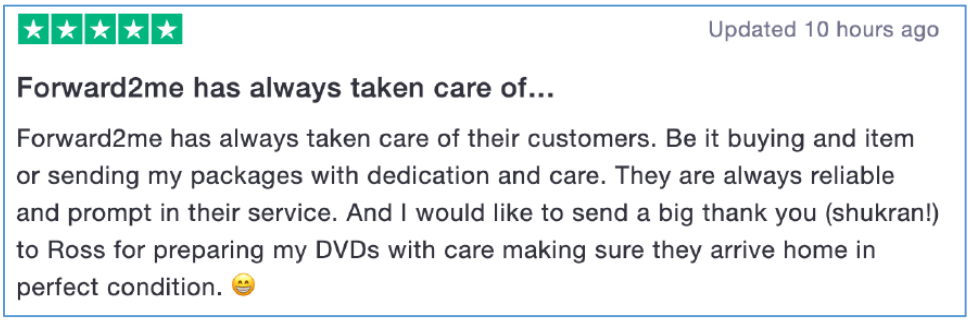
(a)



(b)



(c)



(d)

Figure 1.2 : Examples of Positive Online Reviews

Thus, Type 1 fake reviews provide untruthful information, Written specifically to deceive potential purchasers into endorsing or impeaching a particular item by placing undeserved and/or defamatory reviews.

- Type 2 (Brand Reviewing)

  This kind of reviewing does comment on the 'Brands or Manufacturers' and sound unequivocal about the products, in precise. For example, a review for a specific Amazon product says "I hate amazon, I never buy any of the products sold here". Thus, Type 2 spam reviews focus on specific brands, manufacturers, or e-commerce sites (sellers) as opposed to products. They are generally biased and provide no true benefit to the person who wants to buy that product.

- Type 3 (non-reviews)

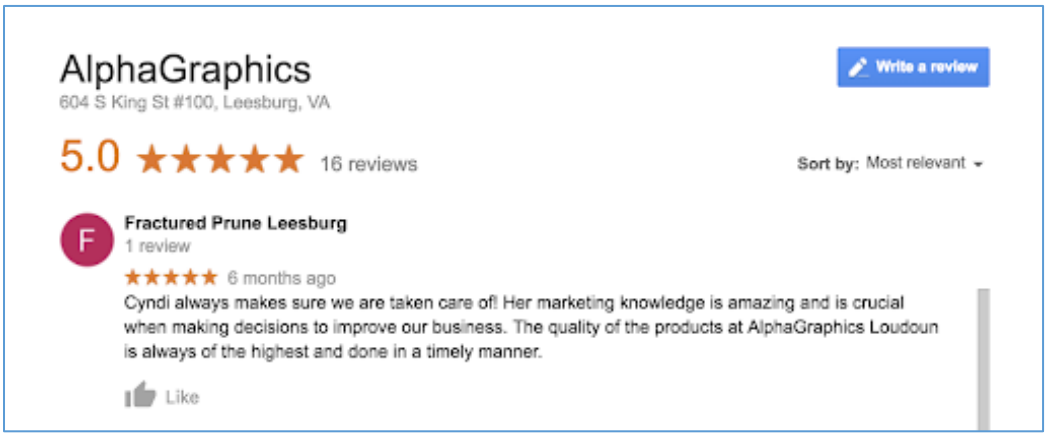
  Type 3 are not actual reviews for real. Prominent use of Type 3 reviews are categorized as, advertisements and irrelevant texts that are considered to bear extraneous questions in addition to random texts.

While developing a spam review system, type 1 spam reviews are more challenging to detect, followed by type 2 and type 3 spams. This research work considers only type 1 and type 2 spam reviews.

1.3. SPAM REVIEWS

By and large, all online businesses continuously implement and monitor methods that can motivate their users to provide positive reviews and in consequence, improve the number of positive business transactions. This conceived substantial unethical and illegitimate activities that manipulated online reviews in a very harmful manner. This fraudulent activity did tend to deceive the opinions which buyers had on the products or brands (Norris *et al.*, 2019). Such reviews, considered to be biased are fabricated and do not provide authentic opinions. Unlike the honest reviewers who genuinely write their reviews on the products, the fake reviewers do it for the financial benefits offered to them by the products' competitors or so. These are termed Spam Reviews and are defined to be deceptive or fictitious reviews that are intentionally forged to look genuine. Some examples of ham and spam reviews are shown in Figures1.3 and 1.4 respectively.

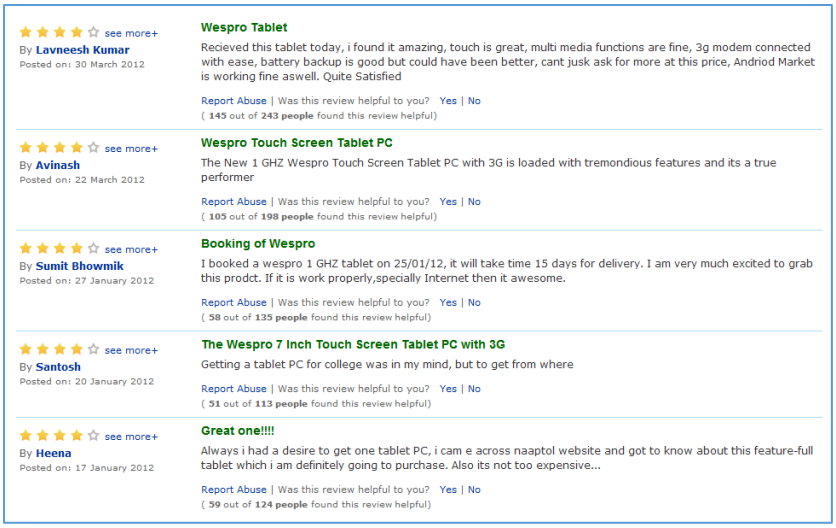
(a)



(b)

(c)

Figure 1.3 : Examples of Ham Online Reviews



(a)

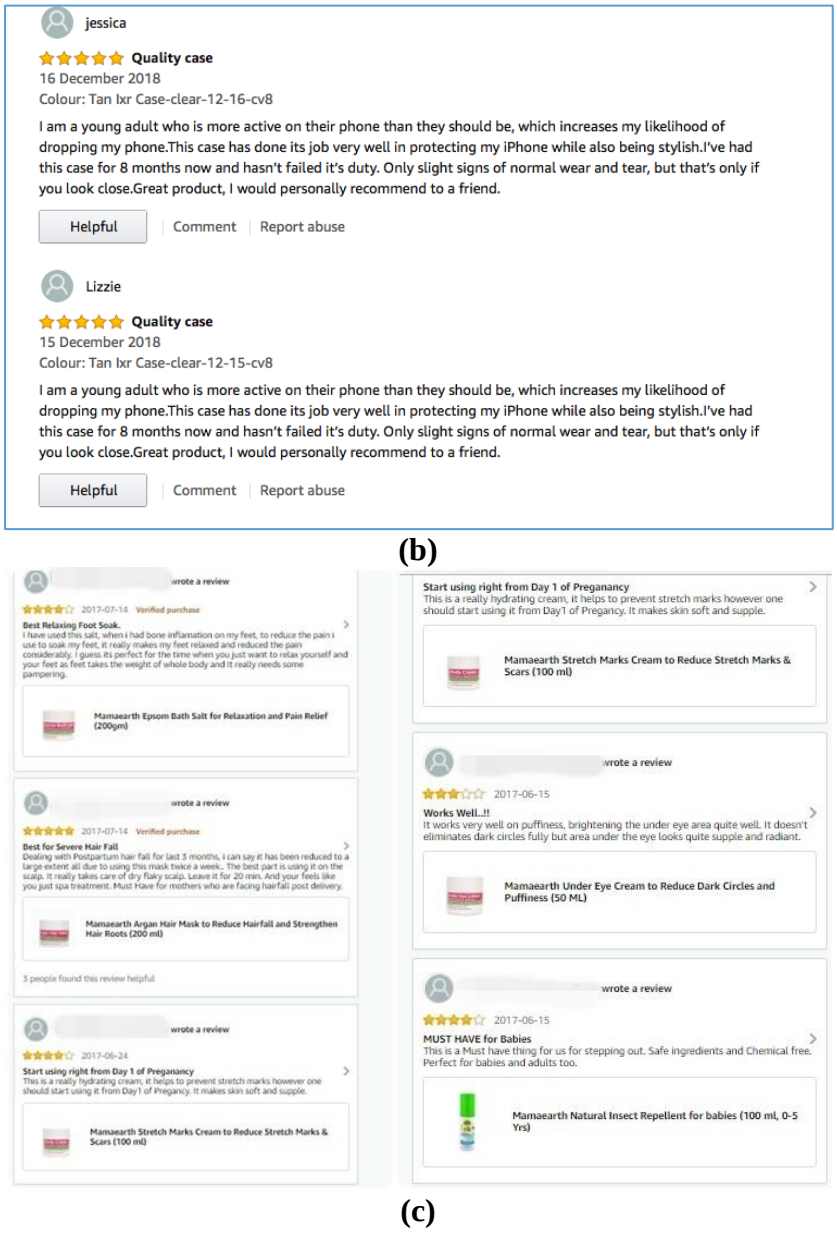


Figure 1.4 : Examples of Spam Online Reviews

Spam reviews were born out of the heavy competitiveness that exists between businesses. As a consequence, some companies, regrettably, employ fake reviewers to promote their product and at the same time, demote the competitor product. Recently, news channels have reported several cases where reviews have been used in a fictitious manner. For example, a chef posted negative reviews on TripAdvisor about the competitor's restaurants (Taylor, 2015). As another example, it was reported that Samsung was fined heavily ($340,300) for employing spammers to write negative fake reviews

about their competitor, HTC Smart phones (Chang, 2013). Recently, BBC News (2021) reported that fake Amazon reviews are being sold in bulk. This news reported that 10 websites were identified to sell fake reviews for products sold in the Amazon market place and charged $5 to $15 per review.

Both positive and negative online reviews can be grouped as genuine or spam. Depending on their employment objective, the spammers create reviews that either increase positive reviews or ascend negative reviews. Fake reviewers write such biased content on their monetary interests and do not provide constructive criticism. Thus, both positive and negative spam reviews can be either ham or spam.

1.3.1. Characteristics of a Spam Review

Fake reviews often have some common features that can be used to detect them. Initially, unverified spam reviews as in reviews written for products that have no proof of purchase, were common. But, today, almost all e-commerce websites are forcing, by default, unverified reviews to the bottom. It is a known fact that customer's span of attention is only on the top few reviews. Thus, this reduces their impact on a purchase decision. However, to circumvent this, spammers buy a product, write a fake review and then return it. Thus, fake reviews may also appear at the top and methods to identify them are very much needed.

The spammers usually write reviews for several products every month and follow identifiable patterns. These patterns indeed are to be identified to remove spam reviews. These patterns are connected to various characteristics and some of them are listed below (Haider, 2020).

(i) Generic tone: The spammers often use a generic tone while writing a review as have very little (or no knowledge) about the technicalities of a product. Hence, they describe the product using terms like "Good", "Superb", "Awesome", "Amazing", "Very very useful", "extremely beneficial", "worth the money", etc. Experience and professional spammers may use words from the product description and often will not add any deeper details.

(i) Review Length: Spammers write either very short text, that is hardly a line or may write lengthy reviews having more than 1 paragraphs. Among these two, short reviews are more common as they do not have any acquaintance with the product and find no time to give away multiple reviews on the same products precisely. Moreover, if they are paid for a quick 5-star rating, which is common, a super short review is what the spammers return.

(ii) Review Rating: People who appoint spammers generally demand spammers to leave a 5-star rating (for products supported by them) or a 1-star rating (competitor's products). These ratings impact the overall rating of a product and therefore, play a crucial role. This feature, if used alone, cannot detect spam reviews, but can be combined with other characteristics.

(iii) Similar Reviews: Many organizations provide a template to the spammers to write fake reviews. So, multiple reviews highlighting same details of products, crafted differently, indicate all of them as spam.

(iv) Broken English: Many spammers are from third-world countries, who do not use English as their first language and hence, many spam reviews have text written in broken English.

(v) Time Stamps: The organizations appoint covey of spammers in sync. They are offered a credit squeeze when appointed, for fabricating 50, 100, or 500 fake reviews on a single product and to post reviews in quick succession. Thereafter, setting "Most Recent" on the review filter and scrolling them, will help to identify many 5-stared (or many 1-stared) reviews posted in a smaller span (usually, 1-2 days). Almost all of these reviews are spam reviews.

(vi) Reviewer's History: Checking on every reviewer's profile seems very difficult. But, if a quick check has to be done for a particular review, the history of the review is very useful in identifying spams. The following points can be checked to determine whether the postings of a reviewer are either spam or not. If the majority of the following list answers a Yes, then the review is spam and cannot be trusted.

- The reviewer has posted reviews consistently. Like, for example, more than five products per week.
- A 5-* or a 1-* rating is always been given away by the reviewer.

- The magnitude of the review is similar for all the reviews posted.
- The review content always upholds a generic tone and does not provide any technical details.

However, the sheer number of online reviews makes it difficult to check the above characteristics. The above discussed characteristics are human friend clues to detect spam, but are hard for machine-based automated systems (Zhang, 2020) and require a different set of characteristics. An example of a review with human-friendly clues for spam identification is shown in Figure 1.5.

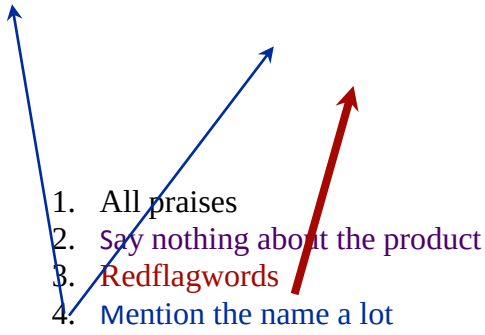


Figure 1.5 : Example of Review With Human-Friendly Clues to Detect Spam

Thus, automated systems for detecting spam reviews are desired. Many online sites are available, which can be used to decide on whether the review is spam or ham. For example, Fakespot (*https://www.fakespot.com)* gives a rating of A to F, with A and B indicating a genuine review. This means that 80% of the reviews submitted to it are reported as spam. Thus, it would still need manual scrutiny. Another example of online spam detection is the review index (https://thereviewindex.com). Review count/reviewer, inactive reviewers, high-velocity reviewers, reviewer history overlap, and unconfirmed review streak are indeed the five factors being used by this system to determine whether the review is ham or spam. This system is more effective in finding spammers than spam reviews. As an outcome, an automated spam review detection system that can improve prediction performance seems to be in high demand.

1.4. SPAMMERS

A spammer is defined as a review author, also called as a reviewer, and is a human who solemnly determine a product or service utilized through originating a review. This reviewer is confederated amidst a set of all reviews banged out by for the identical or distinct products or services during a period of time.

As the process of reviewing a product do not have any scrutiny to analyze its trustworthiness and as reviews can be written and posted by any person, the number of review spams have also increased rapidly. Spammers can be professional or non-professional individuals (Liu, 2015). A professional spammer writes a huge number of reviews and work either as freelancers or as an employee. They get amount for writing reviews. As the number of reviews written by them is high, their behavioural and linguistic patterns can be used to identify their work. Non-professional spammers, on the other hand, are individuals, who write very small number of fake reviews (usually 1 to 3 reviews) and write themfor their personal gain, without any monetary gain. As the number of reviews is small and as they do not follow a common pattern, it is challenging to identify them.

Spammers are hired by other people or businesses can be grouped into two types (Zhang *et al.*, 2018; Xu *et al.*, 2019).

- Individual Spammer: Single person who registers himself/herself multiple times, using different user ids, in single e-commerce site. The spammers belonging to this type, mostly, write only 5-star rated positive reviews. These persons either promote their own products (like a book author promoting his/her book) or write negative or 1-star rated negative reviews about their competitors, but do not write both.
- Group Spammer: Group of spammers, are a set of fraudulent reviewers, who work in collusion, to write lot of reviews (positive or negative) about a product. They are generally appointed to write bulk spam reviews. These types of spammers register in crowd sourcing platforms using multiple user ids to manipulate reviews. Group spammers are the main form of review spamming and are more influential, thus more damaging, when compared to individual spammers.

The reviewsshown in Figure 1.6 are a typical individual spammer example, while reviews in Figure 1.7 shows group spammer reviews.

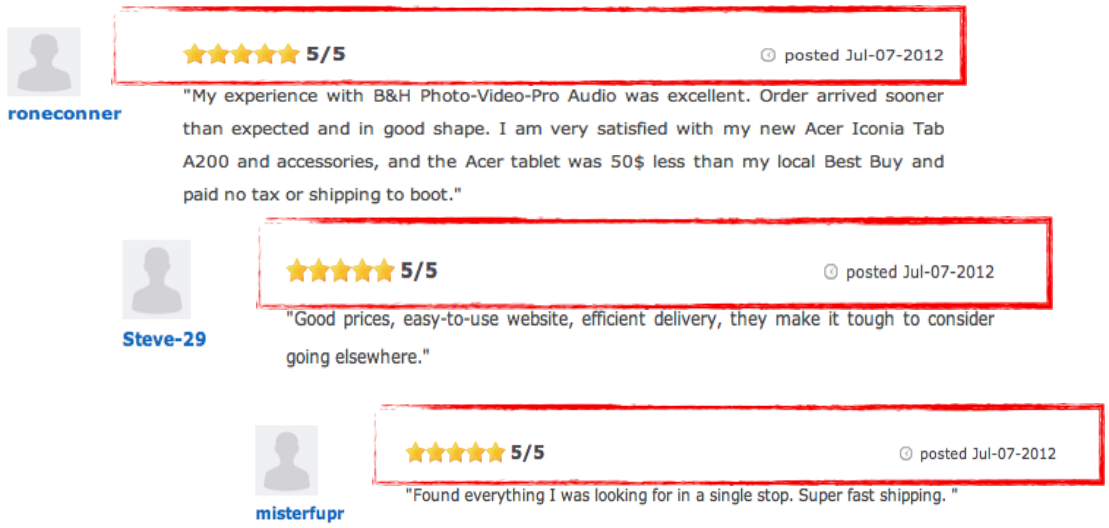


Figure 1.6 : Reviews from Individual Spammer

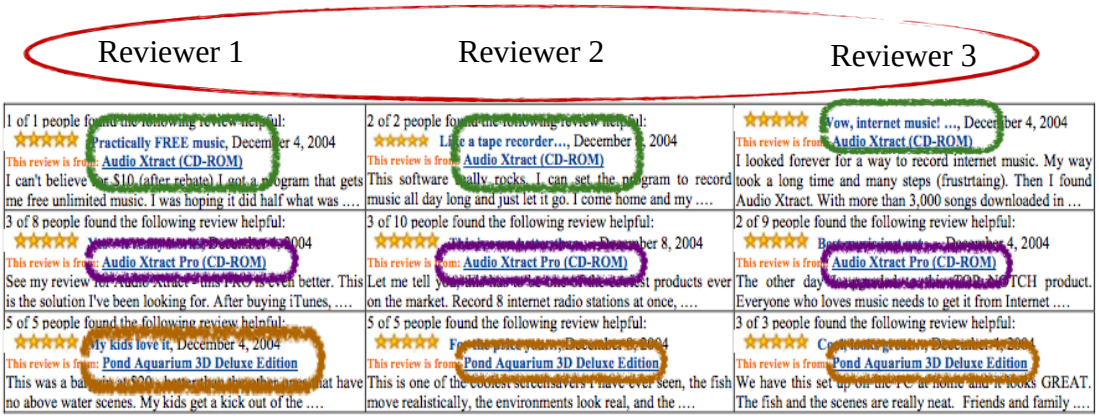


Figure 1.7 : Reviews from Group Spammers

In general, a spam reviewer comes in many forms as listed below.

- The reviewer is a competitor of the product he/she is reviewing. Spamming is done to damage the competitor and help his/her business to grow.
- The reviewer is the owner or an employee or a marketing executive of the business he/she is reviewing. Spamming is done to provide falsified message so as to manipulate public opinion using fictitious positive sentiments.

- The reviewer is an adhoc person who has no previous transactional history with the product he/she is reviewing. Spamming is done to pretend that the person is a consumer in order to promote/demote the business for his/her personal gain.
- The reviewer has some incentive or monetary benefits to write the review. Spamming is done to get this reward and are biased opinions.
- The reviewer violates the guidelines set by the online website where the review is written. Spamming is done as personal attack through hate speech or malicious words.

Spam reviews deceive potential clients, influencing their experience and opinions. A customer motivated to buy a product using these spam reviews, may be dissatisfied. This situation always causes loss of profits and damages the reputation of the brand. Thus, detection and elimination of these spam reviews is a serious concern. The past few years, have envisaged several systems that detect spam reviews. The following section describes the various steps involved.

1.5. SPAM REVIEW DETECTION

The primary objective of the OSRD system is to identify all spam reviews using machine learning algorithms. The OSRD is a tool that implements a machine learning algorithm, A, to decide whether a review, R, is spam or ham (Equation 1.1).

$$A(R,F) = \begin{cases} \text{Spam} & \text{if F has suspicious content} \\ \text{Ham} & \text{otherwise} \end{cases} \quad (1.1)$$

In the above equation, R is the online review that has to be categorized as spam or ham, F is a feature vector that represents the various characteristics of R. It is a common practice to use machine learning techniques (Naem *et al.*, 2018) for spam/ham classification. Thus, the detection algorithm, A, uses a learning algorithm (Θ) to train the machine learning algorithm with the dataset that have features (F) pre-collected from reviews (Equation 1.2)

$$\theta = \Theta(F, C) \quad (1.2)$$

where F ($=\{f_1, \ldots, f_n\}$) and C is the set of target labels, which is {spam, ham} in this research. The detection algorithm, A, handles one review at a time and classifies them as

ham or spam, depending on the result (θ) obtained from (Θ).Two actions are taken from the result (Equation 1.3).

$$\begin{cases} \theta = \text{Ham} & \text{Allow Review} \\ \theta = \text{Spam} & \text{Delete Review} \end{cases} \tag{1.3}$$

Thus, the spam detection system monitors the reviews using two main stages, namely, feature extraction and detection (Mohammad, 2020).

1.5.1. Feature Extraction

Identifying and extracting unique qualities (or features) from each review is the purpose of the feature extraction stage. This stage makes sure that the features extracted provide maximum information regarding a review and have high discriminating capacity. The features extracted are grouped together to form a feature vector, that provides a compressed format of the review and which best describes its whole content.

A set of high-quality factors is important increase spam detection accuracy. A quality feature set consists of relevant and non-redundant features and feature extraction is a process that helps to obtain a representation of a review based on optimal features that can help to improve the detection of spam/ham reviews (Kotsiantis *et al.*, 2006). The feature extraction step is a process that produces a reduced version of the review and is considered important because of the following reasons.

(i) Computational complexity is reduced
(ii) The issue of scalability is handled efficiently
(iii) Improves the machine learning algorithm's generalization ability

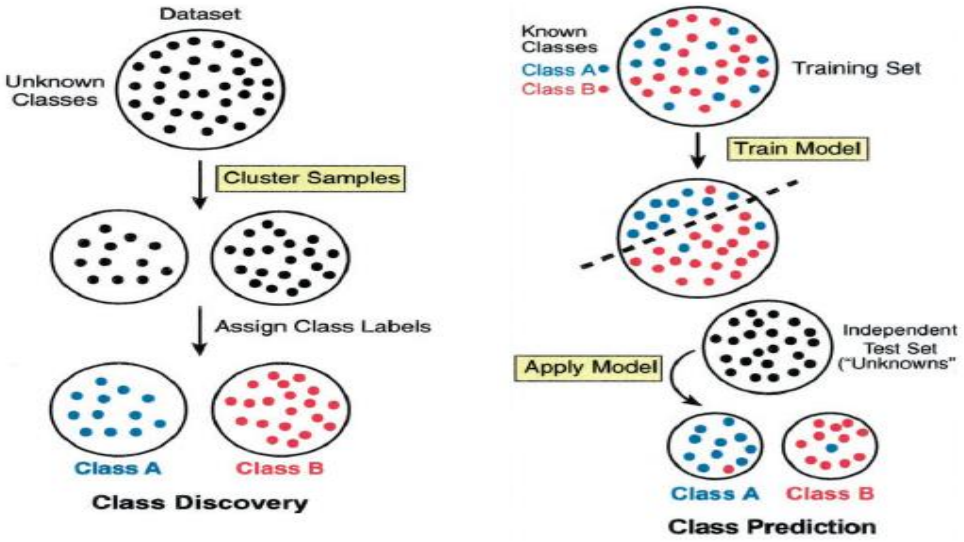
Several types of features can be extracted from an online review, which are grouped into three types as listed below (Dada *et al.*, 2019).

(i) Review Centric Features – These are feature that portray the characteristics of the review and examples include length, time, date, id and rating.
(ii) Reviewer Centric features – These features are used to extract characteristics of the person who wrote the review. Examples include number of reviews, number of positive/negative reviews, deviation rate and content similarity.

(iii) Product Centric Features – These features are used to extract important details about the product being reviewed. Examples include price, rating and sales rank of a product.

1.5.2. Spam Detection

The second stage, detection, decides on whether the review is genuine or fake using the feature vector from stage one. As mentioned earlier, machine learning algorithms are generally adopted in this step, which can be either supervised (or classification) or unsupervised (or clustering) algorithms (Lakshmanaprabu *et al.*, 2018). A Supervised spam detection algorithm is a classification problem that uses a labeled feature set, to separate the reviews into two categories, namely, spam review or ham review (Shahariar *et al.*, 2019).Decision trees, Neural Networks, and Support Vector Machines are examples of classifiers that fall under this category. Unsupervised algorithms, work with an unlabeled feature set and uses similarity measures to group reviews into ham and spam groups (Saumya and Singh, 2020).Hierarchical clustering, K-Means, Self-Organizing Maps, and bi-clustering are examples of unsupervised clustering methods. The main difference between these two machine learning algorithms is presented in Figure 1.8.The steps involved in the conventional OSRD system are shown in Figure 1.9.



(a) Unsupervised Classification **(b) Supervised Classification**

Figure 1.8 : Unsupervised and Supervised Classification

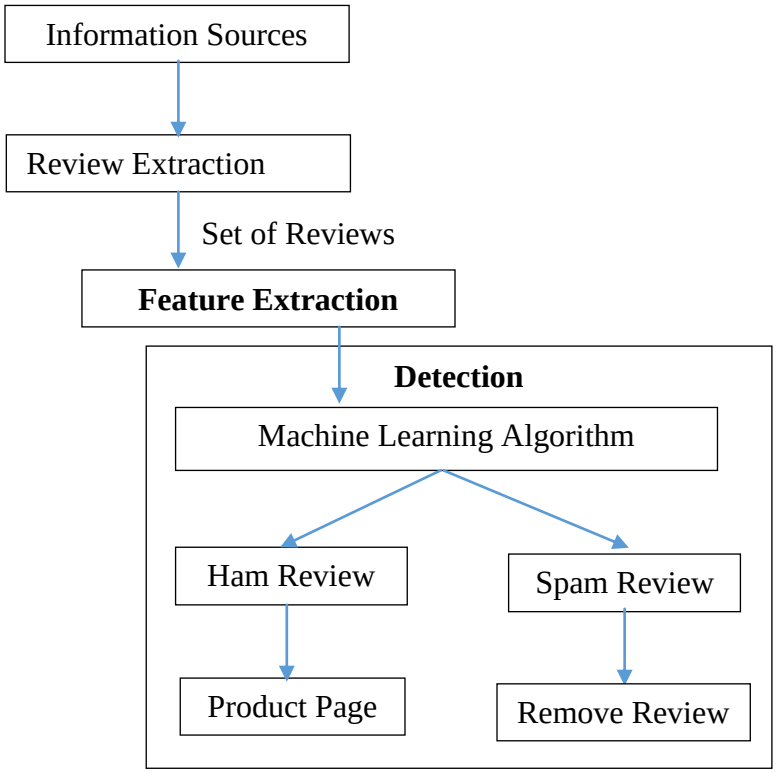


Figure 1.9 : Steps in Review Spam Detection System

1.6. MOTIVATION

Since there are no apparent patterns in the content that can be utilised to establish whether a review is spam or not, detecting spam reviews is a difficult task. Both genuine and false evaluations look very similar, and it takes a lot of work to tell the difference between the two. Automated spam detection systems are in high demand because manual detection is not realistic, not to mention time-consuming, and prone to misidentification.

Even though several OSRD systems have been proposed, a successful system that can meet the three extreme desired features, namely, simplicity (Ease of use), scalability (Work with data of various sizes, from little to large.), and acceptability (produce maximum accuracy), are still a dream. Because this combination is extremely difficult to acquire, this scientific endeavour is another step in the right direction.

Even when faced with a huge volume of online reviews, a wide range of online review content, and a high rate of spammers, an optimal OSRD system can perform well (spammers are normally short lived) (Figure 1.10).Several studies have been carried out to

offer detecting methods that will solve the above-mentioned desirable features as the population grows to design a system that can function effectively under three conditions. Furthermore, existing solutions have a high false-positive rate, a long time to identify spam reviews, a large gap between the installation of spam detection methods and the guarantee of a positive result, and so on.

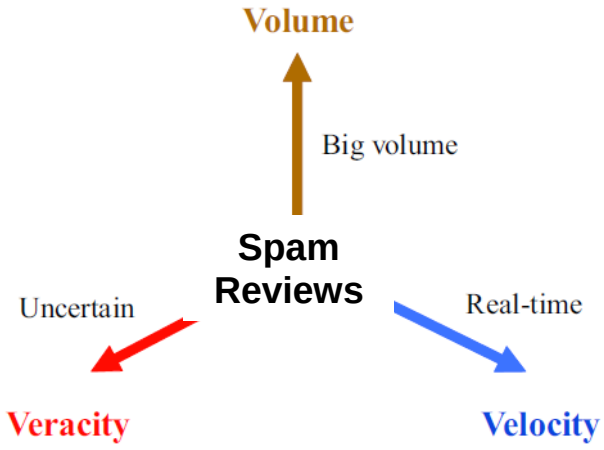


Figure 1.10 : Need For OSRD Systems

Due to the rapid growth in e-commerce sites, the increase in the number of reviews to be analyzed, the innovative methods used by spammers to write fake reviews that look like genuine reviews and the steps that can be further improved to enhance the working of the OSRD system, all motivated this research work to design an OSRD system.

1.7. RESEARCH OBJECTIVES AND PROBLEM STATEMENT

Identifying spam/ham product opinions and reviews is performed using three steps, namely, feature extraction, selection and classification. Various algorithms have been proposed for on each of these steps. However, existing proposals focus on enhancing any one of the steps at a time and only a small number of works have focused on each step and then find methods that effectively integrate the winning methods to form a performance improved system. In short, it is challenging to find an answer to the question "Which is the best algorithm that can be used for each step that when combined improve the performance of the spam identification system ?". This research work attempts to answer the above question and proposes proposes a spam/ham review identification system that first proposes enhanced algorithms to improve the working of each step, from which the

best working method is combined to form the enhanced identification system. To achieve this the research problem is stated as below.

> ***"Given an input online review I_r and a review database $R = \{R_1, \ldots, R_N\}$ having an optimal set of features, F, that has combined review, reviewer and product centric features, along with set of target labels, L= {Spam. Ham}, the research problem is to design enhanced feature engineering and filtering algorithms that can find an accurate target match of Ir in P in an automated fashion that satisfies the three requirements, namely, scalability, high detection rate and high speed".***

To design a system that adheres to the above problem statement, the primary objective of the research work is framed as "to design and implement an Online Review Spam Detection System based on multiple features, enhanced feature selection and hybrid models that combine clustering with classification algorithms, which can help both individuals and businesses to provide a safe and efficient environment during an online purchase".

The specific objectives to meet the primary objectives were framed as follows.

- To perform feature engineering to construct a feature vector having only optimal features extracted from multiple entities, which helps to improve the performance of ham/spam detection systems.
- To design enhanced classification and clustering algorithms to improve the performance of online review spam detection system.
- To design online review spam detection system that combines the two machine learning algorithms (clustering and enhanced classification) to form hybrid models.

1.8. LAYOUT OF THE DISSERTATION

The main goal of this study is to create a method for detecting spam online reviews that is both effective and efficient. This chapter **(Chapter 1, Introduction)** presented the introductory materials covering the various concepts related to online reviews and spam reviews along with the various steps involved in spam detection. The research objectives

along with the problem statement were also presented. The remainder of the thesis is laid out as follows.

The literature review is a critical examination of previous research that is relevant to the job being done. Several proposals for detecting spam reviews have been proposed, and Chapter 2, Review of Literature, provides a critical examination of the available literature that is relevant to the current research activity.

The suggested online review spam detection system is presented in **Chapter 3: Methodology,** which also specifies the major processes. Feature engineering and classification of online reviews as genuine (ham) or fake (spam).were highlighted as milestones in the development of the proposed review spam detection system. This chapter outlines the various algorithms that are enhanced and used in these steps.

Chapter 4, Feature Engineering, deals with algorithms that are used to extracting features from reviews and enhanced methods used to construct optimal feature vectors.

The second step of the spam detection system is a two stage design. The initial stage enhances the working of the machine learning algorithms and the second stage builds a hybrid model that combines the enhanced machine learning algorithm. **Chapter 5, Design of Enhanced SVM Ensemble Classification Model**, focuses on the first stage and proposes an enhanced machine learning classifier based on Support Vector Machine (SVM). The proposed classifier is first improved in its operation and then further improved through the incorporation of ensembling technology, which is explained in this chapter.

The next chapter, **Chapter 6 (Design of Hybrid Classification Systems),** deals with the second stage and presents the method used to construct the hybrid systems that combine the two machine learning methods, classification and clustering along with ensembling technology.

Performance evaluation of the proposed methods and combined online spam review detection system was done through several experiments. These experiments were used to understand the effect of the enhancement methods on spam detection and to study

their cumulative effect on spam detection. In **Chapter 7, Results and Discussion**, the findings are presented and addressed.

Chapter 8, Summary and Conclusion, summarises the study's findings as well as future research directions. Several researchers' work is cited and used as evidence to back up the ideas presented in this thesis. The thesis' **Bibliography** includes a list of each shreds of evidence used.

1.9. CHAPTER SUMMARY

Identification of review spam is difficult, and it necessitates a thorough selection of procedures that can appropriately identify it. This research focuses on developing systems that can improve the performance of existing classification algorithms, especially to improve the accuracy of spam/ham review detection. This chapter presented the fundamental details of review spam detection along with formulated research objectives. A review study was carried out to better understand the current state of spam detection systems, the results of which are reported in Chapter 2, Review of Literature.