
Role of common website features on providing a secure news website: an empirical approach

Mandana Farzaneh*

Department of Information Technology Management,
School of Management,
University of Tehran,
Tehran, Iran
Fax: 0098-021-66427865
E-mail: m.farzaneh@ut.ac.ir
*Corresponding author

Shahriar Mohammadi

Industrial Engineering Department,
K.N. Toosi University of Technology,
Tehran, Iran
E-mail: mohammadi@kntu.ac.ir

Abstract: News websites provide various kinds of information and have a great contribution in creating knowledge to community citizens. Providing security has a great impact on the usability of these websites and encourages users to trust and share their personal information to take advantages of various facilities on the news website. The main contribution of this paper is to examine if website features affect designing a secure news website. The features have been classified by a deep and complete review of the most applicable features in news websites through the study of the top 50 international news websites. Validating the classification was the next step, which was held by identifying experts' opinions about the most pertinent features of news websites that affect the security of the news websites. The aim of this paper is to find out the correlation of each identified feature with each security service. The result would be beneficial for news website's administrators to design these websites effectively and securely in order to satisfy their users by suitable response to their requirements.

Keywords: news website; feature; security; analysing questionnaire; correlation.

Reference to this paper should be made as follows: Farzaneh, M. and Mohammadi, S. (2011) 'Role of common website features on providing a secure news website: an empirical approach', *Int. J. Multimedia Intelligence and Security*, Vol. 2, Nos. 3/4, pp.320–338.

Biographical notes: Mandana Farzaneh is currently a Postgraduate student at the Department of Information Technology Management, School of Management, University of Tehran, Tehran, Iran. She will receive her degree in July 2011. She received her Bachelor degree in Industrial Management from University of Tehran at Iran. She was accepted as one of the 100 top students in Tehran University in 2009.

Shahriar Mohammadi is a former Senior Lecturer at the University of Derby, UK. He also used to be a Network Consultant in the UK for more than 15 years. He is currently a Lecturer in the IT group of Industrial Engineering Department of the University Of K.N. Toosi, of Iran. His main research interests and lectures are in the fields of networking, data security, network security, e-commerce and e-commerce security.

1 Introduction

The critical role of news websites in creating knowledge and consequently improving the quality of life in the global knowledge economy is uncovered to anyone. News is big business today, and as a result, it is an industry, which is now well represented on the web. The web provides a particularly good medium for news that is constantly updateable, enhances the ability to link to information that is more detailed, and facilitates fast, free and convenient access to the latest news. The immense resources of the existing news industry are available to the websites of the leading news services today, which is a good facility for those who like to get their news from the web quickly without any charge. In addition, with the readily updateable nature of the web, all the latest news from around the world is available online almost as soon as it has happened. Because of the demand online, news websites are available in a number of different formats with a number of different focuses. Furthermore, online news is now available to browse, to listen to, to watch, and is readily available in e-mail update form, so users can simply subscribe and get their favourite news in their mailbox (Chen et al., 2011; Xiao, 2009). Therefore, it seems that the web now has covered with the latest generation of news sites.

Making news websites more usable is important to companies. A good news website can keep users from moving away from the website or attract new users, increase its success and enhance several consumer dimensions, including intention to return to the website, trust, and performance improvement (Djamasbi et al., 2010; Hernández et al., 2009; Song et al., 2007). One of the approaches to constitute an effective and a good all-round news website is to focus on the various website features with the aim of responding to various user demands and help them to effectively find out what they need. Neglecting these features would reduce the probability of users to get their desirable outcome of their visits so would diminish their returning to the website as well as their length of use (Barthes, and Tacla; 2002; Chang and Lin, 2003; Chen and Chen, 2008; Ethier, 2008; Guasch and Ugas, 2007; Hernández et al., 2009; Huang et al., 2010; Janssen et al., 2009; Lee and Koubek, 2010; Yang et al., 2010). For this purpose, news websites features should be considered of high priority in designing these websites in order to satisfy users' wants and obtain their satisfaction.

Utilising these features facilitates to provide adaptive and personalise services or information for individual users, and conduct them to find their desired information easily and reliably. This is due to the main objective of these features for designing websites, which is to organise and classify the content, label information, design navigation systems and to help users find their needed information effectively and efficiently. The features help firms to develop a high quality news website and assist users to gain a good grasp of the various kinds of existing news and information. They

have a great impact on tailor to the needs of users and cause to limit the vagueness of non-relevant information for them. Unsuitable use of these features or neglecting them may diminish the probability of returning to the news website by users. Consequently, the proper features of the website ought to be taken into account by the firms in order to improve their capability of enhancing users' probability of return, rate of use, the time spent by them for using the web as well as lock in users and ultimately developing a successful news website. (Chang and Lin, 2003; Chen and Chen, 2008; Choi et al., 2010; Cocquebert et al., 2010; Germanakos et al., 2008; Guasch and Ugas, 2007; Hernández et al., 2009; Janssen et al., 2009; Lee and Koubek, 2010; Su and Kuo, 2010; Telang and Mukhopadhyay, 2005).

Besides the critical role of features in news websites, security is another concern, which these websites are faced. Firms have to pay special attention to creating a secure news website that users are comfort to share their personal information through some features such as mailbox or sign up in order to gain the latest news. Therefore, website features could be considered as one of the most significance approaches to enhance website security from users' viewpoint and enhance their likely of return to the news website. In this regard, it has been an attempt to pay special attention to the associated features of news websites with the intention of providing accurate and reliable information. The main objective of the current paper is to find out the correlation between the news website's features and security. The structure of this paper is as follows: first, it has been tried to detect and classify the most essential and applicable features of news websites. Then the identified features were classified and evaluated by domain experts. They were asked to detect the features, which are critical for designing a secure news websites and have a great impact on promoting the level of security of news website. In addition, they set the priority of security services at the news websites. At last, the experts analyse the features in order to design a news websites with the aim of promoting the level of security and consequently enhancing the value added of news website. The result would be worthwhile for the website administrators and designers to design a news website with high security and effectively and therefore tailor their users.

2 Literature review and hypothesis development

The extension of websites in a distributed environment and shared broadband networks includes real-time data processing, bandwidth, and incorporation of information, raises the issue of personal privacy and security (Doukas et al., 2010; Sioutas et al., 2009). With more and more businesses online and a plethora of applications finding new uses for the internet, security is surely going to be a major concern and one of the most important areas in website and internet services. Security is important to build trust and long-term relationship with users. Internet security measures to deter, prevent, detect, and correct security violation as well as protect data during their transmission and storage over a collection of interconnected networks. Security and privacy structures such as technical standards, security procedures, and protection mechanisms provide content-based privacy assurance, avoid any private information from leaking across the network and enhance the probability of the proper use of consumers' private information. In fact, security is particularly important since users expect that the website would be able to offer a secure networking environment that will protect personal data. They want assurance that their data transmissions are secure, so that their personal information

cannot be intercepted or accessed by unauthorised people (Kapsalis et al., 2006; Lombard and Pietro, 2011; Middleton and Bryne, 2011; Ou and Si, 2010; Paul et al., 2011; Xiao, 2009). Researchers suggest that users will be more inclined to distrust a website when the basic and functional requirements, such as technical aspects, navigation, surfing activity, privacy and security, have not been met (Ou and Si, 2010).

Thus, security has become an inevitable requirement to provide. Security, as part of the system requirements, must be integrated into the system model from the very beginning, if full advantage of model-driven software development is to be taken. However, existing approaches using model-centric development typically ignore security at the modelling stage, rather adding security aspects later in an ad-hoc manner. This can lead to deficiencies in security and more importantly, a less cost-effective development process. The fact that security requirements are usually not considered as an essential part of the overall system requirements is reflected in the fact that design models often describe only what components in a system should do, as in traditional functional requirements. What is equally important is what the systems should not do. Malicious misuse/abuse should be prohibited in the non-functional requirements of security but, unfortunately, the latter is sometimes ignored or considered very late in the system development process. The need of protecting the computers and information that are stored, processed and transmitted are much more important when the information system is web-based and the users utilise internet and websites. Therefore, in recent years, how to produce security is an important research topic and there is an increasing demand for flexible and secure management of websites as a distributed system (Li et al., 2010). In this case, firms should take in to account the importance of security related requirements in early stages of designing websites.

Consequently, finding the potential risk and harm from malicious misuse such as unauthorised access, disruption, as well as developing, implementing, and assessing levels of risk in a website has a great importance. An appropriate website structure must be created to provide security and oversee an effective risk management program (Paquette et al., 2010). For instance, by restricting the access to some pages using back links for security or providing access to some pages in particular order or within specified distance would increase the security of the website (Yen et al., 2007). Indeed, secure and trustworthy service architectures in websites are an immediate requirement to support the huge growth of internet business applications and services. It becomes then crucial to recognise the possible threats and to establish security processes to protect provided services from attacks (Lee and Ahn, 2009; Paul et al., 2011; Yen et al., 2007). For this reason, designing a secure website can be considered as an optimisation problem. Nevertheless, a few studies have been leading toward the design of an efficient security website framework that supports diverse security levels according to a degree of information sensitivity (Taka et al., 2004). Accordingly, the first step involves identifying the various security services that are a somehow a threat to information security.

From a practical perspective, core security services that are often considered part of the taxonomy of website security include integrity, confidentiality and user authentication (Xiao, 2009; Sioutas, 2009). These services enable entities to prove that they are who they claim to be, to be assured that important data has not been altered in any way, and to be convinced that data sent to another entity can be read only by that entity. Organisations can derive tremendous benefits from these services if they consider

security requirements as an essential part of the overall website requirements, just like functional requirements. In this regard, one of the most important security requirements of websites is information security. Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Pulkkinen, 2007). Security services defined by the International Organisation for Standardisation (ISO), include authentication, authorisation (access control), non-repudiation, data confidentiality, and data integrity. These are core principles of information security services which are explained in more detail as follows:

Authentication

The user signs-in once and uses multiple resources after authorisation without the need of multiple sign-ins for authentication and assures that the sender of the message is actually the person he/she claim. Authentication has two-fold. The first one is entity identification that serves simply to identify the specific entity involved, essentially in isolation from any other activity that the entity might want to perform. Therefore, in practice, entity identification generally produces a concrete result that is then used to enable other activities or communications. The second one is data origin identification, which identifies a specific entity as the source or origin of a given piece of data. This is identification with the intent of binding the identified entity to some particular data, regardless of any subsequent activities in which the entity might engage. Such a process can provide support for a non-repudiation service (Adams and Lloyd, 1999). Consequently, in information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important to validate that both parties involved are who they claim they are. Accordingly, enabling the authentication of websites is seen as important to increase trust levels for individuals and businesses dealing with the website.

In this case, passwords are popular and most websites use passwords to authenticate identity although, more sophisticated authentication mechanisms exist, such as smart cards, and fingerprint or iris scans. The main reason is that in many cases passwords are relatively easy to use, easy to administer and provide an acceptable level of security. Password authentication has two main problems. Firstly, users often choose weak passwords and re-use the same password on many separate systems. Secondly, the password has to be entered in full every time the user logs on. Unfortunately, hackers easily misuse them since they can crack simple passwords in minutes. If the passwords are captured, it gives the attacker complete control [Johnston, (2004), p.6]. For example, while logged-in as a normal user, an attacker could impersonate another user on the system and leads to gaining unauthorised access to protected sections of a website. The impact of poor website authentication can be felt in many ways. Some of the potential impacts are as follows:

- users may become the victims of identity theft through providing personal information to a spoofed website
- personal information may be disclosed without user consent
- the attacker can authenticate as the user from another machine on the website

- the attacker obtain a password that can later be used to authenticate as the user; the attacker hijack the user's session by stealing the short-lived session cookie
- the attacker run a malicious program on the client machine that may actively alter requests or perform unwanted requests on behalf of the user who is browsing the web.

Authorisation to resources

The user obtains access to a resource based on local policies or their enforcement and ensures that both parts of the message have the authority to transmit, read, write and delete data on the web. It helps firms to ensure that only authenticated users are allowed the access authorised by the website and that any unwanted or outside access requests are denied (Fu et al., 2001). This is crucial in a distributed network such as websites since entails that user and organisation's private data be secured. In this regard, many websites use of screen shots of the authorisation language displayed to the user on the website and capture how the consumer assents to a transaction by such actions as clicking on an 'I agree' button or entering some digital code or shared secret. Some others maintain audit logs with a date and time-stamp of the consumer's login to include as a method for determining access rights. The general objective of these ways is to demonstrate that the user entered a password and access was verified to the website. Insufficient authorisation leads to an attacker being able to escalate his or her privileges, exercise unauthorised access, and potentially defraud the systems. For example, while logged-in as a normal user, an attacker could gain access to another user's data while still being logged-in under their current account.

Non-repudiation

Intent to accept responsibility of submitting or receiving an electronic message and be bound by its substance. It enables exchanging parties to maintain and revisit the history or sequence of events during a period of transaction. In fact, non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Disputes cannot be resolved unless the evidence has been previously recorded. Consequently, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction (Adams and Lloyd, 1999). Many non-repudiation protocols have recently been designed to assure non-repudiation services. The primary goal of a non-repudiation protocol is to produce the following evidences: non-repudiation with proof of origin; and non-repudiation with proof of delivery. The non-repudiation with proof of origin service provides the recipient of the data with evidence proving that the sender has sent the referenced data at a certain time. It links a message, its originator and its recipient to reuse the same evidence for different messages or recipients. The non-repudiation with proof of delivery service, which is also often called non-repudiation of receipt, provides the sender of the data with evidence that proves that the recipient has received the referenced data at a certain time but it does not prove that the recipient has also processed the data (Wichert et al., 1999).

Consequently, non-repudiation evidence includes the identity of the person intended to receive the proof. For example, with correct non-repudiation evidences, if Alice, denies having sent a message to Bob, or if Bob denies having received it, the non-repudiation of origin, respectively receipt evidences can be presented to an adjudicator, who can evaluate these evidences, in the context they have been generated in, and decide to either accept or reject Alice's and Bob's claims (Kremer and Markowitch, 2003). From a security perspective, there are two things to be considered when websites wants to be assuring of non-repudiation service. The first issue is that if messages at the business level contain confidential information, it is required that no one can read the original messages except the party to which it is sent. Moreover, the second is related to repudiation among parties, which could raise repudiation of recipient (when originator A claims having sent a message to recipient N, who denies having received it) and repudiation of origin (when recipient N claims having received the message from the originator who denies sending it) (Bilal et al., 2005).

Correct non-repudiation evidence provides the following assurances about document transmissions through websites:

- Only the addressee (and no unauthorised users) can read the message. Encryption provides this assurance.
- Data cannot be changed, added, or deleted without the sender's knowledge.
- Parties sending documents are genuinely who they claim to be. Likewise, when those parties receive documents signed by the sender, they can be confident about the source of the documents.
- The parties who send documents cannot readily claim they did not send them. This is referred to as non-repudiation of origin.
- Parties who are sent documents cannot readily claim they did not receive them. This is referred to as non-repudiation of receipt.

Confidentiality

Data should not be disclosed to unauthorised entities. It assures that the communication between authenticated users is not revealed to others, which have not the authority, and therefore unauthorised users read or understand the message. Confidentiality is the assurance of no one may read the data except for the specific entity (or entities) intended. Confidentiality is a requirement that is important when data is stored that can be read by an unauthorised individual, when data is backed up onto a device that can fall into the hands of an unauthorised individual, when data is transmitted over unprotected networks (Adams and Lloyd, 1999). Consequently, confidentiality is the term used to prevent the disclosure of information to unauthorised individuals or systems. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information holds on a system.

Confidentiality examples would be such as storing research data on password protected computers or in locked cabinets or offices, using only encrypted systems for storing research data on laptops, using a code number instead of the participant's real name on study data and blood/tissue samples, and destroying photos, audio tapes, or video tapes (Fu et al., 2001; Bilal et al., 2005; Kremer and Markowitch, 2003).

Furthermore, a piece of information, which is held by users, should only be accessible to the user that requires access to his/her information to perform his job. In this vein, if the exposure of the information could bring embarrassment and heavy penalties, it should be assigned a 'High' rating, to indicate that the confidentiality of this information is extremely important. In addition, if user information has a medium or low confidentiality rating, it is less likely to be targeted than and hence less damage would be done if this data were inadvertently released or was stolen.

Availability

The ratio of the total time a functional unit is capable of being used during a given interval to the length of the interval. It ensures that authorised access to required information would be happen when needed (Kou, 2003). Availability refers to the availability of information resources and represents the requirement that an asset be accessible to authorised person, entity, or device. An information system that is not available when you need it is almost as bad as none at all. Availability means that maintaining 24/7 up time and remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades that is a crucial requirement for websites. Another risk to availability is variability in performance and how the overcapacity threshold is reached. If capacity begins to approach the 80% threshold and compromising some services or performance is necessary, the vendor will most likely protect their own services and pass the degradation in service to their customers. Therefore, for any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. Ensuring availability also involves preventing denial-of-service attacks.

Generally, the more critical a component is, the higher its availability will be. In this case, availability of an organisation's website (which provides authentication services for a high volume of individuals among many websites that are accessible to users), is so important. An interruption in this service could mean the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks. Therefore, a loss of the service could quickly translate into a large financial loss through potential customer loss due to inaccessibility of resources. Because of this, the availability of this websites could be considered 'High'.

Such concerns are still open problems that call for effective and efficient solutions in the website context. It becomes then crucial to develop, implement, and assess various levels of risk as well as recognise the possible threats and establish security processes to protect websites including through these potential risks and harm from unauthorised access or disruption. Consequently, an appropriate website structure must be created to provide security and oversee an effective risk management program (Paquette et al., 2010; Kou, 2003). In this case, the importance of news website features and security services as well encourages the authors to find out the role of the most common and applicable website features on establishing a secure news website. Therefore, because of the website designers concern in designing secure websites and the significance of the news website features; it has been tried to explore the most applicable features that are involved in news websites security. Indeed, the authors believe that if the functional requirements of a website such as its features integrate with the security requirements,

the ability of correct operation of the website (e.g., security) will enhance dramatically. In this regards, the questions of this research that are going to respond is as follows:

- | | |
|---------------------|---|
| Research Question 1 | If website features affect the security of news website. |
| Research Question 2 | What is the priority of security services in news website? |
| Research Question 3 | Which features are recognised as the most influential features on the news websites security? |

3 Investigation of news website's features

Identifying the most basic and applicable news website's features was the first step. There has been an attempt to identify the essential news website's features, which any news website should contains in order to attract users to utilise the website and furthermore, increase the probability of returning to the website. Then, the impact of the identified features in designing and implementing security in news websites has been examined. In this regards, for identifying the essential features of news websites, the list of the top international news websites have been extracted based on the information available in the Alexa website information (<http://www.alexa.com/>). The investigated websites are shown in Appendix 1. Then a profound study of top 50 news websites of international community has been conducted comprehensively in order to extract the most applicable features of this set of websites. Following this step, several features in the news websites have been identified including about us, advertisement, archive, contact us, forum, help, highlight, new, questionnaire, privacy policy, RSS, search, sign up (in), site map, terms and conditions, types of news and useful links.

These features have been assessed then by domain experts with the aim of finding the importance of the features in creating a secure news website. Consequently, a questionnaire was designed and distributed among the experts in order to discover their view about the research questions. The questionnaire contains five questions about the role of each news website features in providing each security services in the form of a Likert scale (1 _ 7). It has been tried to find out the importance of identified feature of news websites on the information security requirements, which is mentioned in the last section with the aim of exploring the logical association between the identified features of news website and security services. Consequently, five questions were set up in a survey questionnaire and then distributed to some domain experts in news industry in order to discover the relationship between important news websites features and the security requirements. The inclusive description of the questionnaire is shown broadly in Appendix 2. The detected website features were further scrutinised by reliable and significance statistical methods in SPSS version 16.0 program in order to realise the most important and usable features for providing a secure news website. It should be noted that all the questionnaires that were sent to the experts were returned. The next step is to determine the reliability of returned questionnaires.

In this regards, the reliability of the questionnaires was investigating by using Cronbach's alpha. Cronbach's alpha measures how well a set of items (or variables) measures a single uni-dimensional latent construct. It provides a measure of the internal consistency of a test or scale and is expressed as a number between 0 and 1. Internal consistency describes the extent to which all the items in a test measure the same concept or construct and hence is connected to the inter-relatedness of the items within

the test. Internal consistency should be determined before a test since it can be employed for research or examination purposes to ensure validity. Accordingly, Cronbach’s alpha as a function of the number of test items and the average inter-correlation among the items is worthwhile in order to determine a research validation (Tavakol and Dennick, 2011). The formula for the standardised Cronbach’s alpha is as follows:

$$a = \frac{N \cdot \bar{r}}{1 + (N - 1) \cdot \bar{r}} \tag{1}$$

here N is equal to the number of items and r -bar is the average inter-item correlation among the items. If the ratio is higher than 0.7, we can be sure that the questionnaire (test) has acceptable reliability. Table 1 shows the result of the reliability statistics of each question that is obtained by investigating the responses of the questions and computed with the above-mentioned software:

Table 1 Cronbach’s alpha

<i>Q1</i>	<i>Q2</i>	<i>Q3</i>	<i>Q4</i>	<i>Q5</i>
0.905	0.894	0.887	0.905	0.883

Considering Table 1, in this exploratory research context, the reliability coefficient of all the data gathered from the questions’ responses had high reliability, which shows that the items of the samples were adequate. Therefore, it would be possible to analyse the questionnaires data with a wide selection of statistical methods in order to answer to current research questions, which they referred to in the previous section. Furthermore, there has been an attempt to realise the association among the features, which could be applicable for each security services. In statistics, a measure of association is a numerical index, which describes the strength or magnitude of a relationship among variables. In this case, dozens of measures exist but they can be categorised into two broad groups: ordinal and nominal. Relationships among nominal variables (such as the current research variables) can be analysed with nominal measures of association such as Pearson’s Correlation Coefficient (Xiong et al., 2004). Investigating the Pearson’s correlation coefficient would help to find out internal relation of features as well as to determine their associations with each security service. This method is obtained by the following formula with the intention of determining the association among news website services:

$$r = \frac{\sum XY - \frac{\sum X \sum Y}{n}}{\sqrt{\left[\sum X^2 - \frac{(\sum X)^2}{n} \right] \left[\sum Y^2 - \frac{(\sum Y)^2}{n} \right]}} \tag{2}$$

where X and Y are considering variables that the correlation between them is measured. To calculate this coefficient, the software was employed and the correlation was calculated where significance is at the 0.01 level (2-tailed). The correlations, which are higher than 0.6 are meaningful and has been considered as high correlation. The results presented in Table 2 indicate the correlation among a set of features (which is shown in the white cells) with the head feature (which is shown in the grey cells) so as to support each security services. Indeed, this test is show whether two variables are connected:

Table 2 Pearson correlation among features

<i>Availability</i>			
Sign up/in	Privacy policy (0.741)	Archive (0.648)	Forum (0.630)
Most visited	Highlight (0.843)	RSS (0.608)	Privacy policy (0.607)
Useful links	Questionnaire (0.765)	Forum (0.644)	
Highlight	Archive (0.716)	Useful links (0.631)	
Search	News classification (0.786)		
About us	Site map (0.820)		
Forum	Questionnaire (0.688)		
<i>Non-repudiation</i>			
RSS	Highlight (0.686)	Search (0.611)	About us (0.616)
	Useful links (0.605)	Questionnaire (0.606)	
Most visited	Highlight (0.679)	Contact us (0.621)	About us (0.601)
	Useful links (0.603)	Questionnaire (0.763)	
Highlight	Advertisement (0.604)	Search (0.632)	Useful links (0.638)
	Questionnaire (0.706)		
Useful links	Search (0.632)	Contact us (0.643)	
Questionnaire	Useful links (0.644)	Terms and condition (0.602)	
Advertisement	Terms and condition (0.603)		
<i>Confidentiality</i>			
RSS	Most visited (0.692)	Highlight (0.766)	Contact us (0.661)
	News classification (0.610)	About us (0.696)	Terms and condition (0.613)
	Useful links (0.646)	Questionnaire (0.623)	
Most visited	Highlight (0.692)	Contact us (0.621)	Useful links (0.678)
Advertisement	Useful links (0.716)	Terms and condition (0.647)	
Useful links	About us (0.645)	Terms and condition (0.604)	Questionnaire (0.624)
News classification	Useful links (0.634)		
<i>Authorisation</i>			
RSS	Highlight (0.669)	Most visited (0.822)	About us (0.699)
	Questionnaire (0.623)	News classification (0.627)	
Most visited	Highlight (0.687)	Questionnaire (0.637)	Site map (0.618)
	Useful links (0.710)	News classification (0.688)	
Highlight	Contact us (0.688)	Useful links (0.655)	About us (0.638)
	News classification (0.697)		
News classification	About us (0.695)	Useful links (0.658)	Questionnaire (0.617)
	Help (0.680)		
About us	Site map (0.673)	Questionnaire (0.666)	Advertisement (0.605)
Useful links	Site map (0.619)	Questionnaire (0.635)	
<i>Authentication</i>			
RSS	Highlight (0.646)	Most visited (0.757)	News classification (0.662)
Most visited	Highlight (0.783)	Useful links (0.654)	
News classification	Highlight (0.724)	About us (0.613)	

In the next step, the identified features of news website that were detected as the main applicable features, were investigated to see if the features have a great contribution on providing security services of news websites. In this regards, binomial non-parametric test was held on the collected data with the aim of identifying the most essential impressive features. The binomial test uses the binomial distribution to decide if the outcome of an experiment in which the count the number of times one of two alternatives has occurred (Abdi, 2007). The binomial distribution is characterised by an event or process where there are two mutually exclusive possible outcomes, such as with the flip of a coin (Spellman et al., 2000). If we arbitrarily define one of those values as a success (e.g., heads = success), then the following formula will tell us the probability of getting k successes from n observations of the random variable when the probability of a success equals p :

$$P(k | n, p) = \binom{n}{k} p^k (1 - p)^{n-k} \tag{3}$$

In present study, success is when test proportion is 0.57142 which means the variables (news website services) that their weight is greater than four from the Likert scale. Moreover, ‘ n ’ was the total number of experts who answer to the questionnaire. Consequently, the feature that their scores are higher than four in the Likert-type scale are the essential features that influence the security of news websites based on domain experts viewpoint. These features are as follows:

Table 3 Binomial test

<i>News website service</i>	<i>Category</i>	<i>N</i>	<i>Observed Prop.</i>	<i>Test Prop.</i>	<i>Asymp. Sig. (2-tailed)</i>	
RSS	Group 1	<= 4	21	0.48	0.5	0.88
	Group 2	> 4	23	0.52		
	Total		44	1		
Highlight	Group 1	<= 4	19	0.43	0.5	0.451
	Group 2	> 4	25	0.57		
	Total		44	1		
New	Group 1	<= 4	19	0.43	0.5	0.451
	Group 2	> 4	25	0.57		
	Total		44	1		
Archive	Group 1	<= 4	27	0.61	0.5	0.174
	Group 2	> 4	17	0.39		
	Total		44	1		
Advertisement	Group 1	<= 4	27	0.61	0.5	0.174
	Group 2	> 4	17	0.39		
	Total		44	1		
Contact us	Group 1	<= 4	28	0.64	0.5	0.096
	Group 2	> 4	16	0.36		
	Total		44	1		

Table 3 Binomial test (continued)

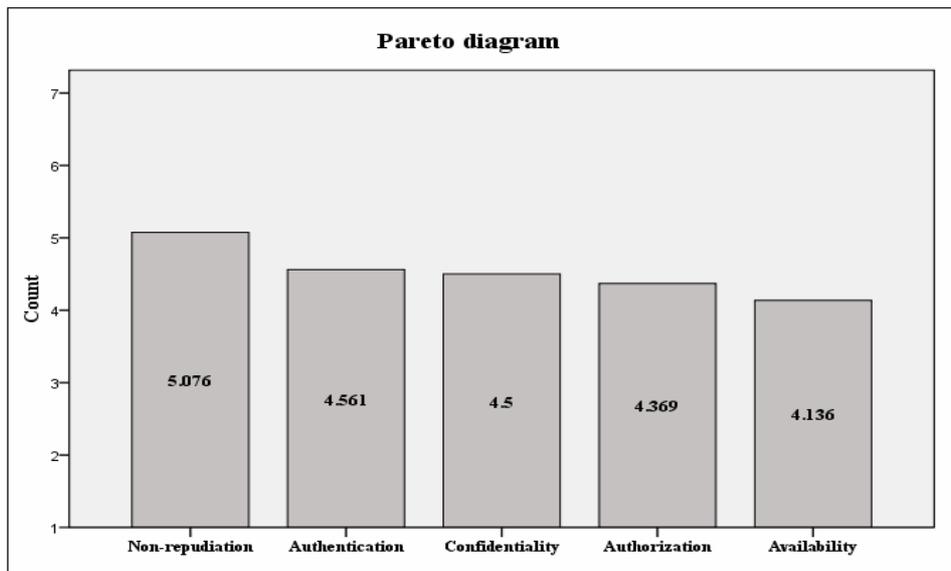
<i>News website service</i>		<i>Category</i>	<i>N</i>	<i>Observed Prop.</i>	<i>Test Prop.</i>	<i>Asymp. Sig. (2-tailed)</i>
Search	Group 1	<= 4	18	0.41	0.5	0.291
	Group 2	> 4	26	0.59		
	Total		44	1		
Type of news	Group 1	<= 4	23	0.52	0.5	0.88
	Group 2	> 4	21	0.48		
	Total		44	1		
About us	Group 1	<= 4	29	0.66	0.5	0.049
	Group 2	> 4	15	0.34		
	Total		44	1		
Site map	Group 1	<= 4	36	0.82	0.5	0
	Group 2	> 4	8	0.18		
	Total		44	1		
Privacy policy	Group 1	<= 4	9	0.2	0.5	0
	Group 2	> 4	35	0.8		
	Total		44	1		
Sign up (in)	Group 1	<= 4	8	0.18	0.5	0
	Group 2	> 4	36	0.82		
	Total		44	1		
Terms and condition	Group 1	<= 4	26	0.59	0.5	0.291
	Group 2	> 4	18	0.41		
	Total		44	1		
Useful links	Group 1	<= 4	25	0.57	0.5	0.451
	Group 2	> 4	19	0.43		
	Total		44	1		
Questionnaire	Group 1	<= 4	23	0.52	0.5	0.88
	Group 2	> 4	21	0.48		
	Total		44	1		
Forum	Group 1	<= 4	23	0.52	0.5	0.88
	Group 2	> 4	21	0.48		
	Total		44	1		
Help	Group 1	<= 4	29	0.66	0.5	0.049
	Group 2	> 4	15	0.34		
	Total		44	1		

In Table 3, the features, which their significance is less than 0.05, are the main features that have a great impact on the security of news websites. Ultimately, five news website features were identified that have contribution on the news website security. These features are as follows:

- about us
- site map
- sign up (in)
- privacy policy
- help.

In the next step the security services was evaluated in order to find out the priority of security services in a news website. In accordance with the responses, the precedence of the security services was detected. Then the importance of sited features in providing the security services has been identified. Figure 1 shows the overall priority of the services with the significance of the five major features to support the security services. The numbers shown in the chart represent the average score of news website features in providing the security services based on the collected data from the survey questionnaires. The result presented in Figure 1 shows the main concern of this paper which clarify the fact that what the role of common website features on providing a secure news website is.

Figure 1 Priority of security services in news website and the role of the most important news website features on them



4 Discussion

Considering the importance of news websites in the information age, various features are required for providing the users with high security. According to this major need, the researchers of this study have done a tremendous effort to study various types of news website features in order to find out the association between the news website security

and the identified features. In this regards, the experts' opinions was collected through a survey questionnaire in order to explore if the features has any contribution in news website security. According to the results of the above tables, it would be concluded that five features are the main news website features related to the security services form the experts' view. Each of these features is linked with a few other features. In other words, each head-feature is associated with a few other sub-features and sequentially they are related to a specific security service.

The result of analysing collected data also shows the role of the most significant news website features identified on the security of these websites. Therefore, in order to increase safety and security of a news website, website administrators should pay attention to the head-features at first and then head over to sub-features. Furthermore, the capability of news websites administrators in designing a secure website would be increase and hence the probability of return, rate of use and the time spent of users would enhance. As mentioned earlier, the security of a website has a significant impact on absorbing and maintaining the current and potential users so the results of this paper would best serve for designing more secure news websites. In addition, the result shows that non-repudiation is the most important security service, among the others in the news website that is supported by the most significant news website's features. In fact, according to the nature of news websites to provide update news from all over the world, which would probably be cited by institutions and individuals, non-repudiation is the most important security services that have a great role on the security level of a news website. Providing this security service effectively would enhance the insurance of information for the website's users. Consequently, these websites are virtual gateways to practically all information regarding the entity it represents and inaccessibility of these services due to security threats – cited in previous sections – may also bring about at least a small level of embarrassment since they relies heavily on the volume of people visiting the website for information provided. Therefore, it reduces consumer confidence, trust and service take-up since the users may be reluctant to migrate to e-services owing to fear of identity theft and other security breaches.

The result of this study guide the academic and industry users to clarify the major news website features related to security services as required in their researches or practical endeavours. In the next step, the result of this study assists in making the way clear for deeper investigations on secure news websites.

5 Conclusions

In recent years, news websites have been one of the main social information systems and are known as a tool for knowledge creation and distribution. The main goal of news websites is to create more value for the citizens through a broad range of accurate and secure functionality as presented in the paper. In this paper, through the pervasive review of the related websites, a comprehensive set of mostly applicable features in news websites have been identified. By investigating through the top international news websites, most frequently useful features have been extracted. Then, the detected features were evaluated by experts to assess and rank the role of the features in promoting the security of news websites. Consequently, the correlation among the news website features and security services has been identified through domain experts' opinions, which has led to identification the role of features in news website security. In addition,

the priority of security services in news website and the role of the major features in providing the services have been detected. The results show that deploying website features concern with news web-based system has advantageous to the firm that extends beyond merely assisting it to response to functional requirements efficiently and effectively. Indeed the features can be used as a security solution on news websites.

The result would be beneficial for other scholars and experts in order to investigate on providing the security services by concentrating on the most significance news website's features. The identified features trigger the mentioned categorisation and guide the academic and industry users to clarify the major uses of news website's features as required in their researches or practical endeavours.

References

- Abdi, H. (2007) 'Binomial distribution: binomial and sign tests', in Salkind, N. (Ed.): *Encyclopedia of Measurement and Statistics*, Vol. 1, Sage, Thousand Oaks, CA.
- Adams, C. and Lloyd, S. (1999) *Understanding Public Key Infrastructure*, MacMillan Technical Publishing, Indiana ZDA.
- Barthes, J-P.A. and Tacla, C.A. (2002) 'Agent – supported portals and KM in complex R&D projects', *Computers in Industry*, Vol. 48, No. 1, pp.3–16.
- Bilal, M., Thomas, J.P., Harrington, P. and Abraham, A. (2005) *NWESP '05 Proceedings of the International Conference on Next Generation Web Services Practices*.
- Chang, C-C. and Lin, I-C. (2003) 'The strategy of reducing the location update traffic using forwarding pointers in virtual layer architecture', *Computer Standards & Interfaces*, Vol. 25, No. 5, pp.501–513.
- Chen, R-C., Bau, C-T. and Yeh, C-J. (2011) 'Merging domain ontologies based on the word net system and fuzzy formal concept analysis techniques', *Applied Soft Computing*, Vol. 11, No. 2, pp.1908–1923.
- Chen, R-S. and Chen, D-K. (2008) 'Apply ontology and agent technology to construct virtual observatory', *Expert Systems with Applications*, Vol. 34, No. 3, pp.2019–2028.
- Choi, B., Hong, J-W., Lee, C. and Lee, H. (2010) 'Deriving web usage strategies for online sales: a decision framework and empirical exploration', *Expert Systems with Applications*, Vol. 37, No. 5, pp.3695–3705.
- Cocquebert, E., Trentesaux, D. and Tahon, C. (2010) 'WISDOM: a website design method based on reusing design and software solutions', *Information and Software Technology*, Vol. 52, No. 12, pp.1272–1285.
- Djamasbi, S., Siegel, M. and Tullis, T. (2010) 'Generation Y, web design, and eye tracking', *International Journal Human-Computer Studies*, Vol. 68, No. 5, pp.307–323.
- Doukas, C., Metsis, V., Becker, E., Le, Z., Makedon, F. and Maglogiannis, I. (2010) 'Digital cities of the future: extending @home assistive technologies for the elderly and the disabled', *Telematics and Informatics*, Vol. 28, No. 3, pp.176–190.
- Ethier, J. (2008) 'Interface design and emotions experienced on B2C websites: empirical testing of a research model', *Computers in Human Behavior*, Vol. 24, No. 7, pp.2771–2791.
- Fu, K., Sit, E., Smith, K. and Feamster, N. (2001) 'Do's and don't's of client authentication on the web', *SSYM'01 Proceedings of the 10th conference on USENIX Security Symposium*.
- Germanakos, P., Tsianos, N., Lekkas, Z., Mourlas, C. and Samaras, G. (2008) 'Capturing essential intrinsic user behavior values for the design of comprehensive web-based personalized environments', *Computers in Human Behavior*, Vol. 24, No. 4, pp.1434–1451.
- Guasch, J.C. and Ugas, L. (2007) 'The digital gap in Maracaibo City in Venezuela', *Telematics and Informatics*, Vol. 24, No. 1, pp.41–47.

- Hernández, B., Jiménez, J. and Martín, M.J. (2009) 'Key website next factors in e-business strategy', *International Journal of Information Management*, Vol. 29, No. 5, pp.362–371.
- Huang, C-C., Liang, W-Y., Lai, Y-H. and Lin, Y-C. (2010) 'The agent-based negotiation process for B2C e-commerce', *Expert Systems with Applications*, Vol. 37, No. 1, pp.348–359.
- Janssen, M., Chun, S.A. and Gil-Garcia, J.R. (2009) 'Building the next generation of digital government infrastructures', *Government Information Quarterly*, Vol. 26, No. 2, pp.233–237.
- Johnston, P. (2004) *Authentication and Session Management on the Web*, SANS Institute.
- Kapsalis, V., Hadellis, L., Karelis, D. and Koubias, S. (2006) 'A dynamic context-aware access control architecture for e-services', *Computers & Security*, Vol. 25, No. 7, pp.507–521.
- Kremer, S. and Markowitch, O. (2003) 'Fair multi-party non-repudiation protocols', *International Journal on Information Security*, Vol. 1, No. 4, pp.223–235.
- Kou, W. (2003) 'Payment technologies for e-commerce', Springer-Verlag, Berlin.
- Lombard, F. and Pietro, R.D. (2011) 'Secure virtualization for cloud computing, in press', *Journal of Network and Computer Applications*, Vol. 34, No. 4, pp.1113–1122.
- Lee, S. and Koubek, R.J. (2010) 'The effects of usability and web design attributes on user preference for e-commerce web sites', *Computers in Industry*, Vol. 61, No. 4, pp.329–341.
- Lee, S. and Ahn, H. (2009) 'Fuzzy cognitive map based on structural equation modeling for the design of controls in business-to-consumer e-commerce web-based systems', *Expert Systems with Applications*, Vol. 36, No. 7, pp.10447–10460.
- Li, J., Huai, J., Hu, C. and Zhu, Y. (2010) 'A secure collaboration service for dynamic virtual organizations', *Information Sciences*, Vol. 180, No. 19, pp.3086–3107.
- Middleton, C.A. and Bryne, A. (2011) 'An exploration of user-generated wireless broadband infrastructures in digital cities', *Telematics and Informatics*, Vol. 28, No. 3, pp.163–175.
- Ou, C.X. and Si, C.L. (2010) 'Consumer trust and distrust: an issue of website design', *International Journal of Human-Computer Studies*, Vol. 68, No. 12, pp.913–934.
- Paquette, S., Jaeger, P.T. and Wilson, S.C. (2010) 'Identifying the security risks associated with governmental use of cloud computing', *Government Information*, Vol. 27, No. 3, pp.245–253.
- Paul, S., Pan, J. and Jain, R. (2011) 'Architectures for the future networks and the next generation Internet: a survey', *Computer Communications*, Vol. 34, No. 1, pp.2–42.
- Pulkkinen, M., Naumenko, A. and Luostarinen, K. (2007) 'Managing information security in a business network of machinery maintenance services business – enterprise architecture as a coordination tool', *The Journal of Systems and Software*, Vol. 80, No. 10, pp.1607–1620.
- Sioutas, S., Sakkopoulos, E., Makris, Ch., Vassiliadi, B., Tsakalidi, A. and Triantafyllou, P. (2009) 'Dynamic web service discovery architecture based on a novel peer based overlay network', *The Journal of Systems and Software*, Vol. 82, No. 5, pp.809–824.
- Song, J., Jones, D. and Gudigantala, N. (2007) 'The effects of incorporating compensatory choice strategies in web-based consumer decision support systems', *Decision Support Systems*, Vol. 43, No. 2, pp.359–374.
- Spellman, R., Johnson, B., Megdal, L. and Feldman S. (2000) 'Measuring market transformation progress & the binomial test: recent experience at Boston gas company', *Proceedings from the 2000 ACEEE Summer Study, American Council for an Energy-Efficient Economy*, Asilomar: CA, pp.6.367–6.378.
- Su, S-F. and Kuo, J. (2010) 'Design and development of web-based information literacy tutorials', *The Journal of Academic Librarianship*, Vol. 36, No. 4, pp.320–328.
- Taka, S., Dixit, S. and Park, E.K. (2004) 'An end-to-end home network security framework', *Computer Communications*, Vol. 27, No. 5, pp.412–422.
- Tavakol, M. and Dennick, R. (2011) 'Making sense of Cronbach's alpha', *International Journal of Medical Education*, Vol. 2, No. 2, pp.53–55.
- Telang, R. and Mukhopadhyay, T. (2005) 'Drivers of web portal use', *Electronic Commerce Research and Applications*, Vol. 4, No. 1, pp.49–65.

- Wichert, M., Ingham, D.B. and Caughey, S.J. (1999) 'Non-repudiation evidence generation for CORBA using XML', In *Proceedings of ACSAC'1999*, pp.320–320.
- Xiao, L. (2009) 'An adaptive security model using agent-oriented MDA', *Information and Software Technology*, Vol. 51, No. 5, pp.933–955.
- Xiong, H., Shekhar, S., Tan, P. and Kumar, V. (2004) 'Exploiting a support-based upper bound of Pearson's correlation coefficient for efficiently identifying strongly correlated pairs', In *ACM SIGKDD*, pp.334–343.
- Yen, B., Hub, P.J-H. and Wanga, M. (2007) 'Toward an analytical approach for effective web site design: a framework for modeling, evaluation and enhancement', *Electronic Commerce Research and Applications*, Vol. 6, No. 2, pp.159–170.
- Yang, Y.J., Sung, T-W., Wu, C. and Chen, H-Y. (2010) 'An agent-based workflow system for enterprise based on FIPA-OS framework', *Expert Systems with Applications*, Vol. 37, No. 1, pp.393–400.

Appendix 1 International news websites

www.signonsandiego.com	www.manoramaonline.com	www.money.cnn.com
www.theaustralian.com.au	www.economist.com	www.reuters.com
www.dailyfinance.com	www.csmonitor.com	www.google.news.com
www.bankrate.com	www.forbes.com	www.weather.com
www.seattlepi.com	www.dnaindia.com	www.usatoday.com
www.denverpost.com	www.wnd.com	www.state.ie
www.sun-sentinel.com	www.miamiherald.com	www.nytimes.com
www.chron.com	www.time.com/time/specials	www.timesplus.co.uk
www.indianexpress.com	www.newsmax.com	www.my.yahoo.com
www.newsnow.co.uk/h	www.newsvine.com	www.wordpress.com
www.startribune.com	www.metafilter.com	www.CNN.com
www.philly.com/?c=n	www.news.sky.com	www.abcnews.go.com
www.azcentral.com	www.associatedcontent.com	www.chicagotribune.com
www.theatlantic.com	www.prnewswire.com	www.cnbc.com
www.ajc.com/?r=t	www.theglobeandmail.com	www.aolnews.com
www.suntimes.com/index.html	www.hindustantimes.com	www.latimes.com
www.newsweek.com	www.businessweek.com	

Appendix 2 Online questionnaire

The questionnaire below has been designed to collect information about evaluating the news website features and their role on security of these websites. These features would be useful to promote the security and safety of news websites. Please answer all questions based on your experience and opinions. Please indicate the number that best matches your opinion for each question (7-item Likert-type scale: from strongly disagree to strongly agree).

Q1 What is the precedence of each security services in a news website?

<i>Security service</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
Authentication: Ensure that the sender of the message is actually the person he/she claims.							
Authorisation: Level of access to a specific resource.							
Non-repudiation: Accept responsibility of submitting or receiving data.							
Confidentiality: Ensure that data not be disclosed to unauthorised entities.							
Availability: The ratio of the total time a functional unit is capable of being used during a specific length of the time.							

Q2 The question below asks you to describe the importance/effect of news website feature on Availability of news websites.

About us, Advertisement, Archive, Contact us, Forum, Help, Highlight, New, Questionnaire, Privacy policy, RSS, Search, Sign up (in), Site map, Terms and conditions, Types of news, Useful links

Q3 The question below ask you to describe the importance/effect of each feature on Non-repudiation of news websites.

About us, Advertisement, Archive, Contact us, Forum, Help, Highlight, New, Questionnaire, Privacy policy, RSS, Search, Sign up (in), Site map, Terms and conditions, Types of news, Useful links

Q4 The question below asks you to describe the importance/effect of each feature on Confidentiality of news websites.

About us, Advertisement, Archive, Contact us, Forum, Help, Highlight, New, Questionnaire, Privacy policy, RSS, Search, Sign up (in), Site map, Terms and conditions, Types of news, Useful links

Q5 The question below asks you to describe the importance/effect of each feature on Authorisation of news websites.

About us, Advertisement, Archive, Contact us, Forum, Help, Highlight, New, Questionnaire, Privacy policy, RSS, Search, Sign up (in), Site map, Terms and conditions, Types of news, Useful links

Q6 The question below asks you to describe the importance/effect of each feature on Authentication of news websites.

About us, Advertisement, Archive, Contact us, Forum, Help, Highlight, New, Questionnaire, Privacy policy, RSS, Search, Sign up (in), Site map, Terms and conditions, Types of news, Useful links