Intelligent based Framework for Detection of Fake News in the Social Network Platforms

Olusanjo Fasola[1], Joseph Ojeniyi[2] and Samuel Oyeniyi[2]
[1]Dominican University, Ibadan, Nigeria
[2]Federal University of Technology, Minna, Nigeria
sanjo.fasola@mbrcomputers.net
ojeniyija@futminna.edu.ng
sammykul01@gmail.com
DOI: 10.34190/ICCWS.20.116

Abstract: Developing a framework for the detection of fake news that is based on a conceptual and intelligent framework will improve the detection of fake news in the social network platforms. It has been hypothesized that if not checked, the increasing spread of fake news may either be the immediate or remote cause of third world war. The existing frameworks suffer in two fundamentals of social concepts and artificial intelligence based revolutionary trends. The focus of this research work is to propose a fake news detection framework that combines the structurally modeled fake news concepts and artificial neural network model. The study used a cross-sectional model testing correlational design which formed the basis of developing the intelligent framework. A simple random sampling technique was used to determine the sample size. The research instrument used was questionnaire administered through Google form survey. The instrument was validated using content, construct and criterion validity. During the pilot test, the reliability of the instrument was established with the standard value of ≥ 0.7 as the benchmark. The method of data analysis used was Pearson Product Moment Correlation Statistics within a significant level of 0.05. Analysis of moment structure tool was used to answer the research hypothesis using structural equation modeling technique. The data obtained from the questionnaires and the test were analyzed using the exploratory factor analysis process (a first generation statistical method of analysis), and the expected designed model, based on Structural Equation Modelling was evaluated using standard goodness of fit indices (GOF) of confirmatory factor analysis (a second generation statistical method of analysis). The dataset generated, measured, analyzed and modeled formed the basis for the development of intelligent based framework. The proposed artificial neural network framework comparatively achieved better detection rates over the conventional and structurally modeled datasets. The framework addresses the social disposition and artificial intelligence based fake news detection gaps.

Keywords: Fake news, information integrity, authenticity, artificial neural network, social network platforms and measurement model

1. Introduction

1.1 Background to the Study

Fake news or junk news or pseudo-news is a type of yellow journalism or propaganda that consists of deliberate disinformation or hoaxes spread via traditional print and broadcast news media or online social media. The false information is often caused by reporters paying sources for stories, an unethical practice called checkbook journalism. Digital news has brought back and increased the usage of fake news, or yellow journalism. The news is then often reverberated as misinformation in social media but occasionally finds its way to the mainstream media as well (Al Asaad and Erascu, 2018; Wang *et al.*, 2019; Zhang and Ghorbani, 2020).

Fake news is a longstanding problem that has affected all types of media: printed media, radio, television and recently digital social media. The "Great Moon Hoax"1 in 1835 is known as one of the earliest examples of fake news, in which the New York Sun published a series of articles about the supposed discovery of life on the moon. Social media is an environment that enables the rapid productions and dissemination of information at a very low cost. Due to its massive dissemination capabilities, digital and social media can reach out to millions of users within minutes. With the increase in popularity, social media has become the main source of information for many people worldwide. Despite these advantages, social media is considered to be the news production media which varies a lot from the traditional news media. Consequently, the quality of information produced by them is considered to be lower than the traditional news media. In digital media, the boundary between news production and information creation is gradually blurring. Due to the low quality of news, there is a need to permanently asses the quality of news published in the social media (Aldwairi and Alwahedi, 2018). Fake news has become increasingly prevalent over the last few years, with over 100 incorrect articles

and rumors spread incessantly just with regard to the 2016 United States presidential election. These fake news articles tend to come from satirical news websites or individual websites with an incentive to propagate false information, either as clickbait or to serve a purpose. Since they typically hope to intentionally promote incorrect information, such articles are quite difficult to detect. In the research titled Detecting fake news in social media network (Aldwairi and Alwahedi, 2018) made use of a tool that can identify and remove fake sites from the results provided to a user by a search engine or a social media news feed (Aldwairi and Alwahedi, 2018). And also (Granik and Mesyura, 2017) showed us in their research that even quite simple artificial intelligence algorithm (such as naive Bayes classifier) may show a good result on such an important problem as fake news classification. Knshnan and Chen, (2018)shows Experimental result on a large miscellaneous events dataset demonstrate the effectiveness of the proposed approach in identifying fake tweets. (Granskogen and Gulla, 2017)wrote a paper focusing on distinguishing satire or parody and fabricated content using the Fake vs Satire public dataset by reviewing existing literature in two phases: characterization and detection.

The challenge of fake news is increasing exponentially because of it low or no technical requirement for its creation, spread, application and/or action. This has led to increasing deception thereby boasting the art of cyberwarfare. Developing a framework for the detection of fake news that is based on a conceptual and intelligent framework will improve the detection of fake news in the social network platforms. It has been hypothesized that if not checked, the increasing spread of fake news may either be the immediate or remote cause of third world war. The existing frameworks suffer in two fundamentals of social concepts and artificial intelligence based revolutionary trends. The aim of this research work is to propose a fake news detection framework based on social concepts and artificial neural network model. In other to achieve the aim, the following objectives were stated:

- To explore the relationship between the relevant social concepts and fake news validity,
- to design a conceptual framework for fake news detection based on the explored relationship,
- to develop a measurement/structural model for fake news detection,
- to evaluate the framework and model for fake news detection,
- to develop an intelligent based fake news detection framework which is trained, tested, validated and evaluated based on the dataset used for validated structural model.

2. Review of related work and theories

The review of the related concepts is based on the fake news components and sub-component divisions. According to the survey of (Zhang and Ghorbani, 2019), holistic components of fake news are: creator and spreader, target victims, social context and news content. The creator and spreader is sub-divided into real human and non-human, target victims sub-divided into potential risk analysis and platform, social context sub-divided into distribution and platform while the sub-components of news content are physical content and non-physical content. Many theories of psychology, theorized well before the advent of social media, seem to explain various aspects of social media behavior quite well. For instance, social comparison on social media can be understood in the context of social comparison theory (Festinger, 1954), rational choice theory (Becker, 1976) and self-determination theory (Deci and Ryan, 1985). These theories have been used in the current study to hypothesize relationship between social media behaviors of consumers and fake news sharing.

2.1 Social comparison theory (SCT)

Social comparison theory (SCT) was formulated to explain how individuals form beliefs and opinions about their capabilities and the drive they possess to evaluate their own abilities (Festinger, 1954). SCT theorizes that, when people are not able to evaluate their abilities on their own, they resort to comparing themselves with others. Such comparison gives them a sense of validation and cognitive clarity. Furthermore, such comparisons produce more accurate assessments when the target of comparison is similar to the person making the comparison. The theory also discusses two types of comparisons, namely, upward and downward comparisons. Festinger (1954) postulated that, when a person is highly motivated, he would tend to engage in upward comparison, that is, compare himself with people who are better than him. This represents the motivation for self-evaluation and self-enhancement. In contrast, an unmotivated person would resort to downward comparison, considering himself to be the best. The behavior of social comparison has been observed to be manifested in social media use also (Nesi and Prinstein, 2015).

2.2 Rational choice theory (RCT):

Rational choice theory has its roots in economics, but is also used by other social scientists to analyze human behavior. The theory postulates that individuals make choices that tend to maximize their personal utility (Becker, 1976). Such choices are in their best self-interest possible and are outcomes of well-thought through alternatives and preferences. The theory also implies that the choices are made in specific context and may change with a change in the situation or beliefs. In a pure economics context, the theory considers rational choice to be the result of analysis of costs and benefits associated with each preference. It has been argued that rational choice theory is also manifested in social media use where consumers consciously decide to continue to use social media, anticipating positive outcomes rather than discontinuing its use on account of social media fatigue (Logan et al., 2018).

2.3 Self-determination theory (SDT):

Self-determination theory provides a framework for the assessment of human motivation and personality (Deci and Ryan, 1985). It posits that people are active organisms who seek to evolve continuously in order to make coherent sense of self. But such natural inclination for growth does not operate automatically and needs social support to catalyze it. An obvious deduction of the theory, then, is that the social context and cultural factors are also capable of impeding the tendencies of psychological growth, initiative and active engagement.

This would detrimentally impact the individual's wellbeing and quality of performance. Conversely, conditions supporting autonomy, competence and relatedness can enhance performance, creativity and diligence. In the context of social media, this theory seems to explain a prominent social media manifestation, FoMO. The need for relatedness and sense of belonging has been argued to be the main motivation driving FoMO (Beyens et al., 2016).

2.4 Social Penetration Theory (SPT)

Social penetration theory seeks to explain the role of information exchange in the development and dissolution of interpersonal relationships. The theory seeks to explain the process of bonding which decides if a relationship is at a superficial level or at an intimate level and how the relationship moves from one level to another (Altman & Taylor, 1973)

As per the theory, the levels of relationships are arranged metaphorically as an ‘onion’, with the outer layer as the least intimate relationship and the inner core as the most intimate relationship. The public image, which is visible to others, forms the outer layer. On the other hand, the private self forms the inner core and it revealed only to significant others over a period through disclosure.

For relationships to develop there must be an exchange of information. Vital to social penetration is breadth, which is the number of topics discussed and depth, which is the degree of intimacy that guides these interactions. Breadth encompasses the variety of topics discussed.

2.5 Social Bond Theory (SBT)

SBT is basically a theory from criminology literature proposed by Hirschi in 1969. SBT describes the social ties an individual has with his group. It says that though a person is naturally inclined towards crime, people with stronger social ties are less interested to indulge in any antisocial or deviant behavior. Four different types of social bonds were defined by Hirschi that ensure socialization i.e. attachment, commitment, involvement and personal norms. Attachment refers to a person’s interest in his/ her social surroundings. Commitment refers to a person’s subjective notion and commitment towards socially accepted goals. Involvement deals with individual’s dealing with conventional activities like family, work, social gatherings. Finally individual with strong personal norms and value systems are less likely to engage in any deviant behavior. In IS literature this theory is mostly used to IS Security literature to understand employee's deviant behavior.

2.6 Social Cognitive Theory (SCgT)

Social cognitive theory provides a framework for understanding, predicting, and changing human behavior. The theory identifies human behavior as an interaction of personal factors, behavior, and the environment (Bandura 1977; Bandura 1986).

In the model, the interaction between the person and behavior involves the influences of a person’s thoughts and actions. The interaction between the person and the environment involves human beliefs and cognitive

competencies that are developed and modified by social influences and structures within the environment. The third interaction, between the environment and behavior, involves a person's behavior determining the aspects of their environment and in turn their behavior is modified by that environment.

According to Jones (1989) "the fact that behavior varies from situation to situation may not necessarily mean that behavior is controlled by situations but rather that the person is construing the situations differently and thus the same set of stimuli may provoke different responses from different people or from the same person at different times."

2.7 Technology Threat Avoidance Theory (TTAT)

Technology Threat Avoidance Theory (TTAT) explains why and how individual IT users engage in threat avoidance behaviors. Unlike most studies that have examined IT security at the organizational level, TTAT provides a framework at the individual user level. The theory has been developed by Liang and Xue by synthesizing the literature from diverse areas including psychology, health care, risk analysis, and information systems. The basic premise of TTAT is that when users perceive that an IT threat exists, they will be motivated to *actively* avoid an IT threat by taking a safeguarding measure if they believe that the threat can be avoided by following the safeguarding measure, or they will passively avoid the threat through emotion-focused coping if they perceive the threat not to be avoidable by any safeguarding measure available to them.

TTAT describes the processes and factors influencing individual users' IT threat avoidance behavior. Drawing on cybernetic theory, TTAT posits that IT threat avoidance behavior can be represented by a cybernetic process in which users intend to enlarge the distance between their current security state and the undesired (unsafe) end state. With the help of coping theory, TTAT submits that users experience two cognitive processes, threat appraisal and coping appraisal. First, users appraise or assess the situation whether the IT threat exists and to what degree it exists. Then they decide what action they will take to avoid it—problem-focused coping and/or emotion-focused coping. TTAT identifies some key factors that explain user perception and motivation in this process. Integrating the literature of risk analysis and health psychology, TTAT suggests that users' threat perception is determined by the perceived probability of the threat's occurrence and the perceived severity of the threat's negative consequences. Based on prior research on health protective behavior and self-efficacy, TTAT proposes that users conceive three factors to assess to what extent the threat can be made avoidable by taking a safeguarding measure—the effectiveness of the safeguarding measure, the costs of the measure, and users' self-efficacy of applying the measure.

2.8 Technology Dominance Theory (TDT)

The Theory of Technology Dominance (TTD) posits that a decision maker may become reliant on an intelligent decision aid under two conditions:

1. The decision maker is low in task experience (see independent factors).
2. The decision maker is high in all factors (task experience, task complexity, decision aid familiarity, and cognitive fit).

According to TDD, reliance on an intelligent decision aid can create a long-term, de-skilling effect in the user as well as hinder that user's growth of knowledge and advancement in his or her domain. Furthermore, TDD states that a negative relationship exists between the user's expertise level and the risk of poor decision making when the expertise of the user and intelligent decision aid are mismatched. When the expertise of the user and the aid are matched, however, a positive relationship exists between reliance on the aid and improved decisions making.

Conceptually, TTD can be divided into three sections which are built on a total of eight testable propositions.

The three sections are:

- Section 1: Addresses the factors that determine the likelihood that a decision maker will rely on an intelligent decision aid.
- Section 2: Addresses the conditions under which a decision maker is vulnerable to being dominated by the intelligent decision aid.
- Section 3: Addresses the long-term impact of intelligent decision aid use on de-skilling domain experts and impeding epistemological evolution.

3. Methodology

The design of the research work is quasi-experimental combining survey and testbed based approach. The population of the study is 387 candidates of cyber security science and information technology security related departments and units. A multistage sampling technique was used to arrive at 120 questionnaires distributed while 94 was responded. Questionnaire was used as the research instruments. The items of the questionnaire were based on the identified component factors of fake news spread. In total 22 items were developed as in Table 1.

Table 1: Measurement Instrument Formation Process

Fake News Main Components	Fake News Sub Components	Construct	Measurement Item	Relevant Theory
Creator/ Spreader	Social bots	Threat perception	Threat perceptions have great impact on user motivation to adopt technology safeguards	TTAT
		Effectiveness of safeguarding measures	Perceptions about safeguard effectiveness impact motivation to adopt the safeguard	
		Decision aid familiarity	Are you always satisfy with the intelligent decision or default recommendation taken by the system for you?	TDT
	Cyborg	Task complexity	Cognitive abilities of your decision making influence reliance on the system intelligent decision for you	TDT
	Benign author & publisher	Deep disclosure	Does in depth share of thoughts influence your intimacy and trust in online information sharing?	SPT
		Commitment & personal norms	Your level of community organization influence obedience to social control	SBT
			Your personal values and belief go a long way to impact your social control	
	Fake news creators	Cognitive fit	In most cases, does the intelligence and smartness in the creation of fakes affect your sense of judgement in distinguishing between the fake news and authentic news	TDT
Target victims	**Role-based analysts**	**Perceived Threat**	**My perception of the susceptibility and severity of malicious IT solutions influence my avoidance**	**TTAT**
	Temporal-based analysis	Shallow disclosure and deep disclosure	The level of my disclosure with the malicious person affects my relationship with such a person	SPT
	Online users	Personal factors and behaviour	My change in behaviour is not easily influenced by external person due to my personal belief and culture	SCgT
	Main streaming users	Attachment, involvement, commitment and personal norms	There is a level I could get to where malicious IT activities cannot influence me	SBT
Social context	Community of users	Attachment, involvement, commitment and personal norms	We could form a cluster of like-minded persons bonded with uniform value beyond reproach	SBT
	Broadcast pattern	Behaviour and environment	Accepted behavioural pattern and environment goes a long way in modelling people's disposition	SCgT
	Main streaming	Effectiveness of safeguarding measures, cost of the measures and	Proper advance knowledge of effectiveness, affordance and efficacy of safeguarding measure greatly influence its deployment	TTAT

Fake News Main Components	Fake News Sub Components	Construct	Measurement Item	Relevant Theory
		user self-efficacy applying the measures		
	Social media	Environment	In as much that humans influence social media, the kind and nature of these media also model our behaviour and negative tendencies	SCgT
News content	New topics	Shallow disclosure	Superficial orientation on a discourse could influence my innocence contribution and sharing	SPT
	Sentiment	Personal factors, behaviour and environment	My judgement of a matter at hand is greatly influenced by personal beliefs and competencies which are constantly being modelled by the environmental social influences and structures	SCgT
	Main purpose	Deep disclosure (Core)	My core knowledge of an event will be a great caution to the disclosure or share of such event	SPT
	Image/video	Task experience, task complexity, decision aid familiarity and cognitive fit	Relay of information with high tech, experience and complexity greatly influence reliance and dominance of such information	TDT
	Body text	Exploratory affective exchange and affective exchange of shallow and deep disclosures respectively	Instant knowledge of a text promptly effect a change in my behaviour or relationship on the text subject matter	SPT
	Headlines	Shallow disclosure	Superficial orientation through news headlines effects spontaneous reaction and change in my relationships	SPT

After a pilot test, the items of the questionnaire were validated appropriately which resulted in the change of some items, some were modified while some remained unchanged. Some selected cyber security experts were used to effect face validity while the construct validity of the questionnaire was also done to provide evidence that the relationships among the items and constructs conform to the requirements. The construct validity of was assessed using parameters from structural equation modelling techniques.

Measure of reliability to be used in this study encompasses internal consistency reliability of the instrument and the composite reliability of the construct. Assessment of the internal consistency of the instrument was carried out using the standardized Cronbach's Alpha reliability technique. Measuring the internal consistency reliability involves measuring two different versions of the same item within the same test based on the correlations between different items. The composite reliability is computed from data in multiple variables in order to derive reliable and valid measures of latent, theoretical constructs. Values greater than 0.7 for Cronbach's Alpha and Composite reliability are generally accepted to reveal higher level reliability of the instrument and the construct respectively.

The reliability coefficient (alpha Cronbach) of the questionnaire for each component factors was computed and the values fell within acceptable range of 0.619 to 0.889.

A 22-item questionnaire using online google form was used to collect the research data from the targeted audience using. The data obtained from the questionnaire was analyzed using the exploratory factor analysis process (a first generation statistical method of analysis), and the expected designed model, based on

Structural Equation modelling was evaluated using standard goodness of fit indices (GOF) of confirmatory factor analysis (a second generation statistical method of analysis). The GOF included Chi-Squares/degree of freedom, average variance extracted, composite reliability, root mean square error of approximation, comparative fit indices and standard factor loading greater than 0.5 baseline.

4. Results and discussion

4.1 Descriptive statistics results

The descriptive statistics of the measured variables was also computed and the values for mean, standard deviation, variance, skewness and kurtosis were within acceptable ranges.

4.2 Correlation of the factors results

The correlation of the four component factors of fake news are presented in Table 2, Table 3, Table 4 and Table 5.

Table 2: Correlation for creator/spreader based factors

Correlations

		SBTP	SBESM	SBDAF	CBTC	BAPDD	BAPCPN1	BAPCPN2	FNCCF
SBTP	Pearson Correlation	1	-.129	.051	.078	-.024	.023	.089	-.116
	Sig. (2-tailed)		.215	.626	.454	.819	.827	.392	.267
	Sum of Squares and Cross-products	123.319	-17.213	6.574	11.702	-2.830	1.915	10.191	-12.362
	Covariance	1.326	-.185	.071	.126	-.030	.021	.110	-.133
	N	94	94	94	94	94	94	94	94
SBESM	Pearson Correlation	-.129	1	.148	-.108	-.101	-.119	-.078	-.034
	Sig. (2-tailed)	.215		.156	.301	.332	.254	.455	.745
	Sum of Squares and Cross-products	-17.213	144.309	20.617	-17.468	-12.947	-10.777	-9.628	-3.926
	Covariance	-.185	1.552	.222	-.188	-.139	-.116	-.104	-.042
	N	94	94	94	94	94	94	94	94
SBDAF	Pearson Correlation	.051	.148	1	-.057	-.007	-.086	.023	-.240*
	Sig. (2-tailed)	.626	.156		.585	.945	.410	.826	.020
	Sum of Squares and Cross-products	6.574	20.617	135.234	-8.936	-.894	-7.553	2.745	-26.851
	Covariance	.071	.222	1.454	-.096	-.010	-.081	.030	-.289
	N	94	94	94	94	94	94	94	94
CBTC	Pearson Correlation	.078	-.108	-.057	1	-.003	.061	-.180	.011
	Sig. (2-tailed)	.454	.301	.585		.977	.559	.082	.918
	Sum of Squares and Cross-products	11.702	-17.468	-8.936	181.745	-.426	6.213	-24.979	1.404
	Covariance	.126	-.188	-.096	1.954	-.005	.067	-.269	.015
	N	94	94	94	94	94	94	94	94
BAPDD	Pearson Correlation	-.024	-.101	-.007	-.003	1	.056	-.044	-.080
	Sig. (2-tailed)	.819	.332	.945	.977		.590	.675	.446
	Sum of Squares and Cross-products	-2.830	-12.947	-.894	-.426	113.457	4.521	-4.798	-8.160
	Covariance	-.030	-.139	-.010	-.005	1.220	.049	-.052	-.088
	N	94	94	94	94	94	94	94	94
BAPCPN1	Pearson Correlation	.023	-.119	-.086	.061	.056	1	.099	.211*
	Sig. (2-tailed)	.827	.254	.410	.559	.590		.344	.041
	Sum of Squares and Cross-products	1.915	-10.777	-7.553	6.213	4.521	56.989	7.649	15.330
	Covariance	.021	-.116	-.081	.067	.049	.613	.082	.165
	N	94	94	94	94	94	94	94	94
BAPCPN2	Pearson Correlation	.089	-.078	.023	-.180	-.044	.099	1	-.102
	Sig. (2-tailed)	.392	.455	.826	.082	.675	.344		.327
	Sum of Squares and Cross-products	10.191	-9.628	2.745	-24.979	-4.798	7.649	105.415	-10.117

Correlations

		SBTP	SBESM	SBDAF	CBTC	BAPDD	BAPCPN 1	BAPCPN2	FNCCF
	Covariance	.110	-.104	.030	-.269	-.052	.082	1.133	-.109
	N	94	94	94	94	94	94	94	94
FNCCF	Pearson Correlation	-.116	-.034	-.240*	.011	-.080	.211*	-.102	1
	Sig. (2-tailed)	.267	.745	.020	.918	.446	.041	.327	
	Sum of Squares and Cross-products	-12.362	-3.926	-26.851	1.404	-8.160	15.330	-10.117	92.777
	Covariance	-.133	-.042	-.289	.015	-.088	.165	-.109	.998
	N	94	94	94	94	94	94	94	94

*. Correlation is significant at the 0.05 level (2-tailed).

Table 3: Target victim correlations

Correlations

		RBAPT	TBASDDD	OUPFB	MSUA
RBAPT	Pearson Correlation	1	-.275**	-.251*	.202
	Sig. (2-tailed)		.007	.015	.051
	Sum of Squares and Cross-products	103.926	-29.617	-30.223	26.234
	Covariance	1.117	-.318	-.325	.282
	N	94	94	94	94
TBASDDD	Pearson Correlation	-.275**	1	.033	-.219*
	Sig. (2-tailed)	.007		.750	.034
	Sum of Squares and Cross-products	-29.617	111.745	4.149	-29.489
	Covariance	-.318	1.202	.045	-.317
	N	94	94	94	94
OUPFB	Pearson Correlation	-.251*	.033	1	-.155
	Sig. (2-tailed)	.015	.750		.137
	Sum of Squares and Cross-products	-30.223	4.149	139.330	-23.298
	Covariance	-.325	.045	1.498	-.251
	N	94	94	94	94
MSUA	Pearson Correlation	.202	-.219*	-.155	1
	Sig. (2-tailed)	.051	.034	.137	
	Sum of Squares and Cross-products	26.234	-29.489	-23.298	162.979
	Covariance	.282	-.317	-.251	1.752
	N	94	94	94	94

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4: Social context correlations

Correlations

		CUA	BPBE	MSE	SME
CUA	Pearson Correlation	1	-.207*	.082	-.034
	Sig. (2-tailed)		.045	.430	.747
	Sum of Squares and Cross-products	160.053	-29.830	11.096	-4.596
	Covariance	1.721	-.321	.119	-.049
	N	94	94	94	94
BPBE	Pearson Correlation	-.207*	1	-.073	-.099
	Sig. (2-tailed)	.045		.482	.344
	Sum of Squares and Cross-products	-29.830	129.745	-8.894	-12.106
	Covariance	-.321	1.395	-.096	-.130
	N	94	94	94	94
MSE	Pearson Correlation	.082	-.073	1	.211*

Correlations

		CUA	BPBE	MSE	SME
	Sig. (2-tailed)	.430	.482		.042
	Sum of Squares and Cross-products	11.096	-8.894	113.372	24.128
	Covariance	.119	-.096	1.219	.259
	N	94	94	94	94
SME	Pearson Correlation	-.034	-.099	.211*	1
	Sig. (2-tailed)	.747	.344	.042	
	Sum of Squares and Cross-products	-4.596	-12.106	24.128	115.872
	Covariance	-.049	-.130	.259	1.246
	N	94	94	94	94

*. Correlation is significant at the 0.05 level (2-tailed).

Table 5: News content correlations

Correlations

		NTSD	SP	MPDD	IVT	BTE	HSD
NTSD	Pearson Correlation	1	.063	-.027	.083	-.032	.116
	Sig. (2-tailed)		.547	.796	.428	.759	.266
	Sum of Squares and Cross-products	174.553	8.383	-3.936	13.617	-4.596	17.809
	Covariance	1.877	.090	-.042	.146	-.049	.191
	N	94	94	94	94	94	94
SP	Pearson Correlation	.063	1	.078	.040	-.004	.034
	Sig. (2-tailed)	.547		.456	.702	.966	.743
	Sum of Squares and Cross-products	8.383	101.957	8.660	5.043	-.489	4.021
	Covariance	.090	1.096	.093	.054	-.005	.043
	N	94	94	94	94	94	94
MPDD	Pearson Correlation	-.027	.078	1	.002	.085	.040
	Sig. (2-tailed)	.796	.456		.981	.418	.700
	Sum of Squares and Cross-products	-3.936	8.660	121.277	.340	10.085	5.170
	Covariance	-.042	.093	1.304	.004	.108	.056
	N	94	94	94	94	94	94
IVT	Pearson Correlation	.083	.040	.002	1	-.037	-.117
	Sig. (2-tailed)	.428	.702	.981		.723	.260
	Sum of Squares and Cross-products	13.617	5.043	.340	155.457	-5.011	-17.021
	Covariance	.146	.054	.004	1.672	-.054	-.183
	N	94	94	94	94	94	94
BTE	Pearson Correlation	-.032	-.004	.085	-.037	1	-.034
	Sig. (2-tailed)	.759	.966	.418	.723		.747
	Sum of Squares and Cross-products	-4.596	-.489	10.085	-5.011	117.372	-4.255
	Covariance	-.049	-.005	.108	-.054	1.262	-.046
	N	94	94	94	94	94	94
HSD	Pearson Correlation	.116	.034	.040	-.117	-.034	1
	Sig. (2-tailed)	.266	.743	.700	.260	.747	
	Sum of Squares and Cross-products	17.809	4.021	5.170	-17.021	-4.255	135.489
	Covariance	.191	.043	.056	-.183	-.046	1.457
	N	94	94	94	94	94	94

4.3 Structure of Measurement Model and Structural Equation Model

The structure of the measurement model and structural model is shown in Figure 1. The latent variables are creator/spreader, target victim, social context and news content. They form the basis of Intelligent based framework in section 4.4. This structure also forms a good and robust framework for building effective dataset

for the detection of fake news which combines the fundamental concepts of fake news in terms of the source, social context and social content.

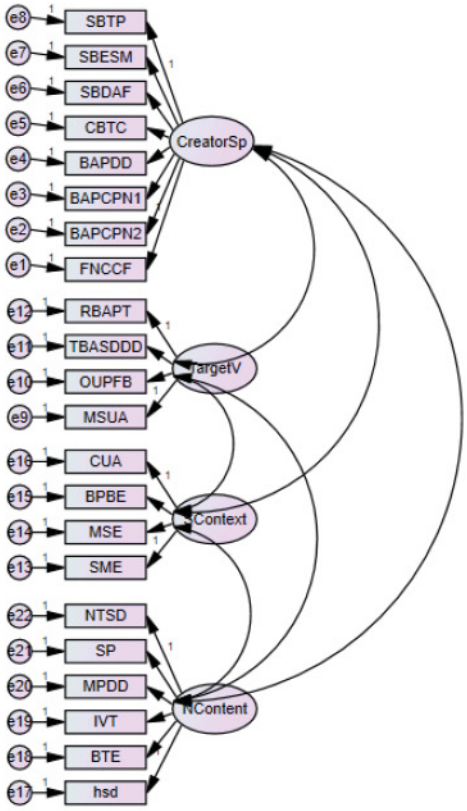

Figure 1: Measurement model

4.4 Artificial Neural Network based Framework for Fake News Detection

The structure of the proposed intelligent based approach using artificial neural network is shown in Figure 2.

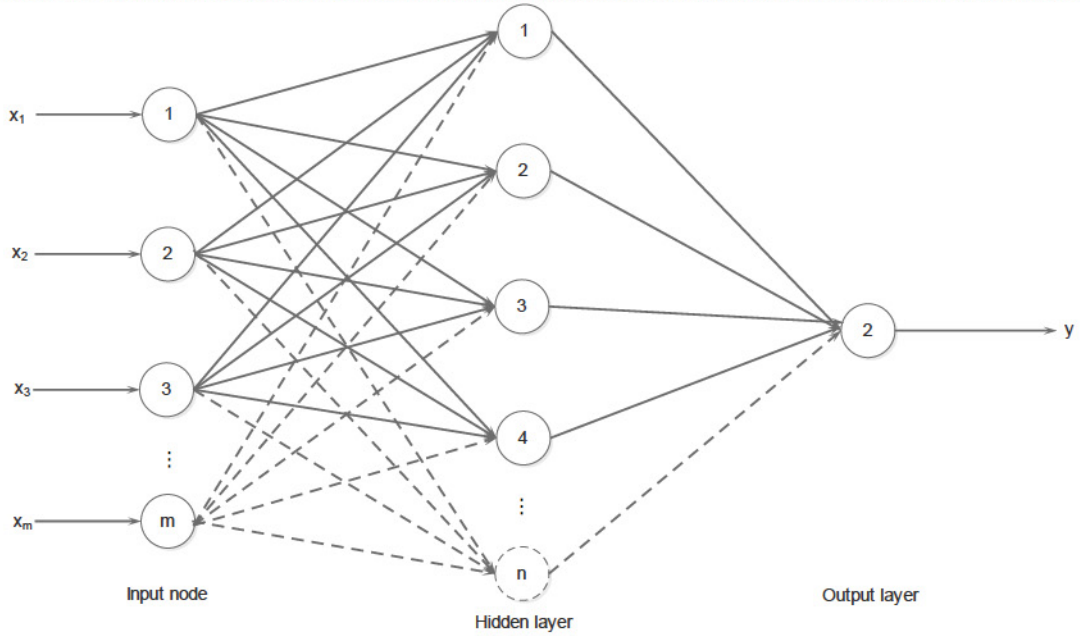

Figure 2: Artificial Neural Network based Architecture for Fake News Detection

The values of x_1, x_2, ..., x_n takes on the attributes of creator/spreader, target victims, social context and news content while y gives assertive values for either fake news or not.

4.5 Discussion and evaluation of results

The fitness of the proposed model was evaluated based on the examination of the Goodness-of-Fit-Statistics (GFI), the Chi-square to the degree of freedom (CMIN/DF), Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), and Root-Mean-Square Error of Approximation (RMSEA). The evaluation thumb rule was based the definition by Hair et al. (2010). The results obtained from the measurement model for the factors statisfy the thumb rule for the goodness of fit indices. The value obtained for CMIN/DF is 1.9 81 which is lesser than th,e thumb rule of <=3.000, CFI is 0.950 against the thumb rule of (>=0.920), RMSEA is 0.032 against the rule of (<=0.070), TLI of 0.954 against the thumb rule of (>0.90) and GFI of 0.961 against the thumb rule of (>0.90). From the result of the unstandardized regression weight, most of the observable correlations were statistically significant. This substantially indicates that the features based on these variables will improve supervised learning framework of artificial neural network. From the prototypic implementations, the following average performance of fake detection was achieved: accuracy (98.11%), sensitivity (97.91%) and specificity of 98.2%.

5. Conclusion

Fake news has become a societal menace capable of causing unimaginable havoc. Different interdisciplinary approaches are required to curb it growing trends. Solid and research-based frameworks like the one proposed in this work is needed to serve as a good foundation for subsequent studies. In order to achieve better results, further survey and experimentations is recommended.

Acknowledgements

The researchers wish to acknowledge the efforts of the department of Cyber Security Science of Federal University of Technology Minna for making their Digital Forensic Laboratory available to the researchers for some bench work. Also worthy to be mentioned is the MBR Computer Consultants for providing a high configuration testbed for the data analysis.

References

Aldwairi, M. and Alwahedi, A. (2018) 'Detecting fake news in social media networks', *Procedia Computer Science*. Elsevier B.V., 141, pp. 215–222. doi: 10.1016/j.procs.2018.10.171.

Al Asaad, B. and Erascu, M. (2018) 'A tool for fake news detection', *Proceedings - 2018 20th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2018*. IEEE, pp. 379–386. doi: 10.1109/SYNASC.2018.00064.

Granik, M. and Mesyura, V. (2017) 'Fake news detection using naive Bayes classifier', in *2017 IEEE 1st Ukraine Conference on Electrical and Computer Engineering, UKRCON 2017 - Proceedings*, pp. 900–903. doi: 10.1109/UKRCON.2017.8100379.

Granskogen, T. and Gulla, J. A. (2017) 'Fake news detection: Network data from social media used to predict fakes', *CEUR Workshop Proceedings*, 2041(1), pp. 59–66.

Knshnan, S. and Chen, M. (2018) 'Identifying tweets with fake news', *Proceedings - 2018 IEEE 19th International Conference on Information Reuse and Integration for Data Science, IRI 2018*, 67, pp. 460–464. doi: 10.1109/IRI.2018.00073.

Wang, Y. *et al.* (2019) 'Systematic Literature Review on the Spread of Health-related Misinformation on Social Media', *Social Science and Medicine*. Elsevier, 240(August), p. 112552. doi: 10.1016/j.socscimed.2019.112552.

Zhang, X. and Ghorbani, A. A. (2019) 'An overview of online fake news: Characterization, detection, and discussion', *Information Processing and Management*. Elsevier, (March), pp. 1–26. doi: 10.1016/j.ipm.2019.03.004.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R.E.,(2010). Multivariate Data Analysis, 7th Edition. Pearson: US

Zhang, X and Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. Information Process and Management, 57(2), 1- 26.

Festinger, L., (1954). A theory of social comparison processes. Hum. Relat. 7 (2), 117–140

Becker, G.S., (1976). The Economic Approach to Human Behaviour. University of Chicago Press, Chicago and London.

Deci, E.L., and Ryan, R.M., (1985). Intrinsic Motivation and Self-Determination in Human Behavior. Plenum Press, New York, NY.

Nesi, J., and Prinstein, M.J., (2015). Using social media for social comparison and feedback- seeking: gender and popularity moderate associations with depressive symptoms. J. Abnorm. Child Psychol. 43 (8), 1427–1438. https://doi.org/10.1007/s10802-015- 0020-0.

Logan, K., Bright, L.F., and Grau, S.L., (2018). Unfriend me, please!: social media fatigue and the theory of rational choice. J. Mark. Theory Pract. 26 (4), 357–367. https://doi. org/10.1080/10696679.2018.1488219.

Beyens, I., Frison, E., Eggermont, S., 2016. I don't want to miss a thing: adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress. Comput. Hum. Behav. 64, 1–8. https://doi.org/10.1016/j. chb.2016.05.083.

Taylor, D. A., & Altman, I. (1975). Self-disclosure as a function of reward-cost outcomes. *Sociometry*, 18-31.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Mustafa Canan is Assistant Professor in the Department of Information Sciences at the Naval Postgraduate School. Research focuses on decision making, information operations, situational awareness, implicit cognition, and human-machine teams. He was a National Research Council (NRC) Postdoctoral Fellow at the Air Force Research Laboratory at Wright-Patterson AFB. He holds Ph.D. degrees in Particle Physics and Engineering Management. Dr. Canan teaches decision making in complex situations, and project management, and has published articles in Nature, Nature Communication, IEEE, and other leading journals and conferences.

Joel Coffman is an Assistant Professor in the Department of Computer and Cyber Sciences at the US Air Force Academy. He received his BS from Furman University and his MS and a PhD from the University of Virginia, all in computer science. Joel's research interests include automated software diversity, cloud security, and keyword search in databases.

David Crow is working towards a Master of Science in Computer Science at the Air Force Institute of Technology in Dayton, Ohio. His research concerns vehicle security using such tools as deep learning and empirical dynamic modeling. David completed a Bachelor of Science in Computer Science at the Missouri University of Science and Technology.

Martina J. Z. de Barros received her Master Degree in Distributed Systems Engineering from the Dresden University of Technology in March 2014. Currently, she is a PhD Student at Technical University of Dresden. Prior to that, Martina received a Bachelor degree in Computer Science from Pedagogical University in Mozambique.

James DeMuth is a wargame and exercise designer at the National Defense University's Center for Applied Strategic Learning. He joined the Center in November, 2015 after receiving his B.A. in International Affairs from the Elliott School at George Washington University. He primarily focuses on the creation of educational wargames for senior-level military and government officials.

Chuck Easttom, D.Sc. is a researcher with 27 published books, over 60 published papers, and 17 patents. He conducts research in cyber warfare, engineering, cryptography, applied mathematics and other areas. He holds advanced degrees in cyber security, systems engineering, and applied computer science.

Margus Ernits is CTO of RangeForce where he is the architect of a cloud based e-learning platform that supports simulating cyber attacks in complex networks for hands-on, gamified and adaptive learning. Margus has been awarded three times as a Lecturer of the Year in Estonian IT College

Olusanjo O. Fasola, is a Senior Lecturer and Head of Department of Physical and Mathematical Sciences at Dominican University, Ibadan, Nigeria. He has a PhD in Artificial Intelligence with many publications in reputable journals. He is engaged in a several high impact industrial collaborations and linkages.

Mr. Kieran Fletcher is recent graduate of National Intelligence University (NIU)'s Masters of Science and Technology Intelligence program. While studying at NIU Fletcher developed an interest in cyber-security application of machine learning.

Dr. Guillermo A. Francia, III's research interests include industrial control systems and vehicular network security. He is a two-time Fulbright award recipient and is the 2018 winner of an Innovation in Cybersecurity Education award. He holds a Distinguished Professor Emeritus position at Jacksonville State University and serves as Faculty Scholar at University of West Florida.

Petr Frantis is an associated professor at the University of Defence in Brno, Czech Republic. He received his MSc degree in computer sciences from Military Academy in Brno and a Ph.D. degree from University of Defence. He currently works as deputy chief of Department of Informatics and Cybernetic Security. His main research areas are simulations, synthetic environments, and cybersecurity.

Fernando Garcia-Granados is a recent graduate in Cyber Security from Tallinn University of Technology and Tartu University whose studies and research focused on how to best educate senior leaders in information security. Currently, he is an Information Security Analyst in Los Angeles.