

Validation of the toolkit for fake news awareness in social media

Mahmood A. Al-Shareeda¹, Murtaja Ali Saare², Selvakumar Manickam¹, Shankar Karuppayah¹

¹National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

²Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

Article Info

Article history:

Received Oct 16, 2022

Revised Mar 30, 2023

Accepted Apr 2, 2023

Keywords:

Fake news

Fake news awareness

Social media

Social media based toolkit

Toolkit

Validation of the toolkit

ABSTRACT

Fake news has gained attention in recent years, particularly among social media users. The quick spread of fake news has been made possible by the increased usage of social media as a platform to get the most recent news and information. As a consequence, it is getting harder to distinguish between real news and fake news. This essay will outline a study that evaluated the usefulness of a toolset for identifying false news. The first hypothesis is that an increase in media literacy will result in a rise in awareness of fake news. The second theory is that fake news toolkits significantly increase students' and working adults' awareness of false news. On the staff of a manufacturing company and an institution, a survey was undertaken. The organization's employees were given approximately 150 questionnaires, and 110 responses were received. The project includes the creation of a web application-a fake news awareness toolkit-that will raise user awareness of fake news in terms of knowledge, behaviour, and attitude among students and workers.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia

11800 USM, Penang, Malaysia

Email: selva@usm.my

1. INTRODUCTION

Although not recent, the term “fake news” gained popularity after the 2016 US presidential election, which caught the attention of academics and general consumers [1]-[4]. According to a research, 62 percent of its inhabitants access news on social media sites rather than on traditional mediums. The most popular social media channel at the time for disseminating false information was Facebook, and the majority of people tended to accept the information that flowed favouring Donald Trump over Hillary Clinton [5]-[7]. Fraudulent news is a story that has been made up and widely disseminated via social media, the phone, and chat messages in an effort to obtain political warning or influence from anyone who typically has evil intents and propagandist messages [8]-[11]. Authors of fake news waste a lot of time researching social and political events on numerous networking sites [12]-[14].

Due to the low cost of producing news content, social media is mostly used as a news distribution channel. Publishers use false information as a “tool” to make quick money [15]-[17]. Nowadays, bogus news thrives on social media platform. In conclusion, fake news is rapidly gaining ground and could do more harm if it is not curbed soon. Therefore, raising people's knowledge of fake news is essential so that they can appreciate the significance of reducing it [18]-[21].

The following inquiries are what this study aims to answer: i) RQ_1 : according to knowledge, behav-

ior, and attitude, what amount of awareness is there?; and ii) RQ_2 : how can a false news awareness toolkit raise people's awareness of it?. The following are the primary goals of this study: i) O_1 : to create a false news awareness toolbox that could increase public awareness of fake news; and ii) O_2 : to assess the toolkit's success in raising public awareness of fake news. The following hypotheses are those that will be explored in this study based on the previously mentioned objectives: i) H_1 : a rise in media literacy affects the level of awareness of fake news; and ii) H_2 : the fake news toolkit significantly raises public awareness of fake news.

Therefore, it is crucial to assess people's perceptions and understanding in order to continue researching fake news awareness and educating the public. A toolset will help individuals understand fake news better and respond to it media literately. This can help to address the aforementioned problems and curb the spread of false information. The major significant contributions of this work are summaries as follows.

- This study will benefit academics who want to learn more about raising organisational and institutional levels of awareness of fake news.
- This study aims to provide light on how false news may have an adverse effect on people, society, and organisations.
- The first web application or toolkit for fake news awareness has just been created. Therefore, it is really hoped that this toolkit would be useful to everyone in the world, not just the study's participants.
- Finally, this toolkit's main contribution is to lessen the country's harmful effects of fake news.

The rest of this paper is constructed as follows. Section 2 reviews some related work for fake news awareness in social media. Section 3 provides background of this paper in detail. Section 4 shows the description of the research design, toolkit, and data analysis. Section 5 shows the process of the implementation of the toolkit. Section 6 provides results and analysis. Finally, the conclusion and recommendation and future work of this paper are provided in section 7 and section 8, respectively.

2. RELATED WORK

In this section, we describe and compare some related work for fake news awareness in social media. Table 1 summarizes the four main related works the methodology used in their work is the quantitative method. These four works are as follows.

Table 1. Summary of four main related works

Author	Findings	Limitations
Surjandy <i>et al.</i> [22]	University students who play video games conducted a poll to learn how they use their smartphones to spread fake news	i) in order to lessen the harmful effects of fake news, the study did not include any courses on fake news awareness or teaching university students about fake news; and ii) given the approach used, the data's interpretation was constrained.
Baharum <i>et al.</i> [23]	i) utilizing an application to give visitors to the Mount Kinabalu Botanical Garden information on the plant species found in Kinabalu Park; and ii) mobile applications are a superior way than educational programmes since they may deliver facts to all kinds of people and are not constrained by time or place.	The usefulness of the app produced in raising public knowledge of biodiversity was not a focus of this study. No post-test information is gathered following user use of the application.
Peker <i>et al.</i> [24]	i) analyzed preventative strategies and talked about the methods used by mobile social networks to distribute fake news; ii) a new time classification was unveiled to stop the spread of false information; and iii) the issue of the spread of incorrect information was discussed in terms of workable solutions.	i) the methods utilised reduced the data's ability to be interpreted; and ii) results have not been exhaustive; rather, they constitute a series of noteworthy examples of a method to stop the spread of fake news.
Campan <i>et al.</i> [25]	i) a module for cybersecurity awareness was suggested by research, with its main attributes setting it apart from some other modules; ii) the study contributes to greater understanding of cybersecurity. After completing the CSAM, 323 participants (or 76.3% of participants) reported having a greater understanding of cybersecurity.	i) only college and high school students were included in the research, and organisations are more likely to have high user numbers and cybersecurity risks; ii) to make reading easier for readers, the data was not graphical presented effectively. Due to the search and selection procedure, the results were limited; and iii) the use of research methodologies, such as quantitative or qualitative methods, is not emphasised in the study.
Ahmed <i>et al.</i> [26]	i) the survey question "Security, awareness, and incident reporting" forms the basis of the research strategy; and ii) four categories make up the survey: incident reporting, cybersecurity practises, cybersecurity awareness, and demographics.	i) need to recommend developing a unique cyber awareness framework in conjunction with mobile technology; and ii) the study was constrained by the literature choice.

Surjandy *et al.* [22] looked into the ways in which university students who play video games use their smartphones to spread false information and how aware they are of it. In their work, the research found new findings in terms of gender and academic rank game players of college students with dissemination and awareness of fake news, despite the fact that the 25 questioners were directly distributed to university students at random and statistical descriptive explanatory analysis was used to show university students' activities. Baharum *et al.* [23] created the "Ikimono Mikke" smartphone app to raise awareness of biodiversity. Users of this app will be able to learn more about the plant species found at Mount Kinabalu Botanical Garden and Kinabalu Park. The Mount Kinabalu Botanical Garden and Kinabalu Park's flora images can also be contributed by users. In order to create a module that will assist students to become more aware of security issues, Peker *et al.* [24] set out to understand the present level of security awareness among college and high school students. To achieve the objectives of the common internet/technology users, Peker *et al.* [24] created a survey with pre-and post-tests and distributed it to students on our campus and at nearby high schools. Campan *et al.* [25] addressed the role that current social network technologies, such as influence maximization, information diffusion, and epidemiological models, play in the production and dissemination of fake news. Ahmed *et al.* [26] presented an extensive survey on Bangladeshi citizens' knowledge of cybercrime. To perform this study, versions of the survey that were both online and offline were developed. According to the survey, there is an unsatisfactory and patchy awareness level. The general public is uninformed of accepted cybersecurity standards.

3. BACKGROUND

3.1. Fake news definition and types

Fake news was recently defined as "intended and verifiably false news articles which misinform the audience" [5], [27]-[29]. Due to its interruptive and disappointing nature, as alleged by scientists and professionals, the term "fake news" has garnered somewhat less attention [30], [31]. The most prevalent type of shaming is political, along with false reports based on crimes and misrepresented real-world events. Satire, parody, fabrication, manipulation, advertisement, and propaganda are six techniques used to operationalize false news in previous studies.

- Hoaxes: the readers of hoax news were led to assume that the stories they were reading were true, when in fact the pieces were just fake news. Hoaxes are rumours that are spread through social media and employ actual facts to give the message a confident appearance. A hoax can actually harm another person [2], [32]-[34].
- Parody: the use of non-factual facts to add humour and a presentation style that mimics traditional news media distinguish parody news from satire news [27], [35].
- Photo manipulation: it is considered fabricated news when real photos or videos are exploited to support false claims. Whereas preceding classes often linked to text-based objects, this categorization defines graphic information [7], [36].
- Advertisement: advertisements for fake news may mimic legitimate news articles and make reference to press releases that have already been published [37].
- Fabrication: news that aims to draw people in order to benefit the individual or boost traffic. A fabricated example is "clickbait." [38], [39].
- Satire: satire is hilarious news that is intended to amuse readers and is presented in a mocking style similar to that of mainstream media. It uses exaggerated comedy to amuse the general public while providing news updates [40].

4. METHOD

4.1. Research design

The following steps highlight the several sequential components that make up the overall study methodology: i) analyse the existing body of knowledge in the topic; ii) questions are examined and modified if required; iii) an online survey tool is used to distribute all the questions; iv) the present study and literature analysis serve as the foundation for the quantitative data collection; v) users must utilise the created tools; vi) a post-survey was done to gauge the usefulness of the toolkit that was created; vii) data analysis that is analytical and statistical; viii) discussion of the results; and ix) findings and conclusions.

4.1.1. Pre and post test

The term “pre- and post-test” refers to a research strategy that is also known as “pre-experimental” or “before and after.” The flowchart for how this study is carried out, from the survey and data collecting through the assessment of the toolkit’s effectiveness. Figure 1 shows the research design of the paper. This step is very important to achieve in the system.

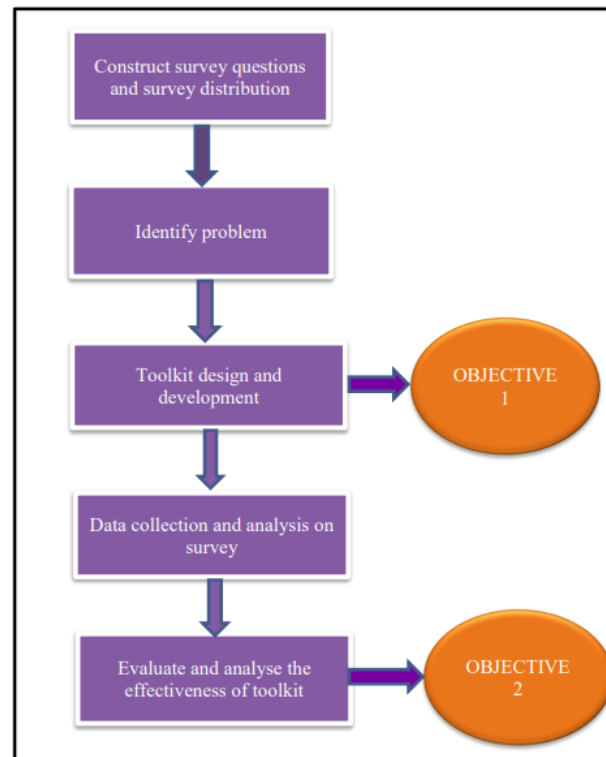


Figure 1. Research design

4.1.2. Pre and post survey on fake news awareness

Google form is generated with 25 questions about how people use and understand media related to fake news. This questionnaire’s responses will be used to gather data for the study. The questions’ overarching strategy is based on the prior measurement and methodology. i) 6 questions about demographics; ii) 4 multiple-choice questions about media literacy or knowledge; iii) 4 behavioural questions; and iv) 11 attitude-related questions. In order to collect 110 responses, the questionnaire was distributed to two distinct sites, first in a manufacturing company and then in a local institution. The data was analysed after receiving the 100 responses. The presurvey gauges respondents’ level of perception of current false news, and the postsurvey gauges the efficiency of the fake news awareness toolbox.

4.2. Toolkit

The goal of the suggested toolkit is to assist people in becoming more aware of fake news, particularly in relation to how to differentiate between authentic and unauthentic sources, and to prevent the spread of misleading news that contributes to public confusion and misinformation. The web app’s objectives are: i) to observe trends in people’s knowledge of bogus news before finishing the toolbox and ii) to assess and contrast how well the toolkit approach works at raising public awareness of false news.

4.2.1. Question design

The questionnaire is divided into 4 sub-sections. containing two sections: section A of the form asks demographic questions, and section B is divided into three sections: knowledge, behaviour, and attitude, as shown in Figure 2.

- Demographics: basic demographic questions are asked in this section. Gender, age, educational attainment, employment status, principal news source, and media platforms were among the inquiries made.
- Knowledge: this category is crucial to the study since it corresponds to knowledge of fake news. It was questioned whether people were familiar with the term “fake news.” The purpose of the knowledge-based inquiry is to ascertain whether the respondents are aware of the veracity of the news on the current website for fact-checking.
- Behavior: the respondents’ attitudes about current news sources and current events are the focus of this section. The behaviour of respondents when reading the news and using the internet was evaluated as part of the attitude’s dimension.
- Attitude: the assessment of respondents’ knowledge of fake news and their background was the main emphasis of this section. Regard was paid to how people would react to false information, as well as how confident and trusting they were of the news they read.

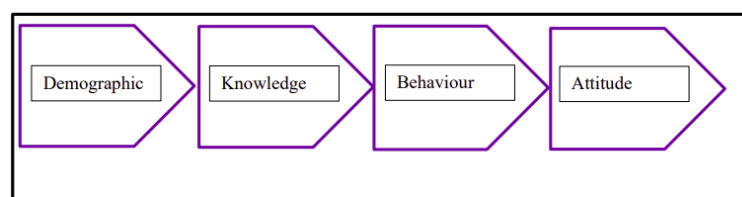


Figure 2. Questions design

4.2.2. Research approach

There are two sorts of research methodology: qualitative and quantitative technique approaches. Research objectives are met using a quantitative technique. data gathering using a quantitative and data analysis are described. The description of these approaches is as follows:

A. Data gathering using a quantitative approach

This study uses quantitative methodology to assess how well-informed people are about fake news in organisations and institutions. Each question’s survey data is tallied and displayed as pie charts or graphs. This information will be gathered and assessed. In order to ascertain people’s knowledge and perception of fake media, 110 respondents will react to 25 questions.

B. Data analysis

Software for data analysis using statistics this study makes use of statistical package for data science (SPSS). It was created by the IBM Corporation and is frequently used by academics and researchers around the world. A very user-friendly statistics tool that may be applied to a variety of statistical tests. This statistical application performs comparison and correlation statistical studies in conjunction with univariate, bivariate, and multivariate procedures in both parametric and nonparametric statistical methods.

To get the best outcomes for the intended application and study objectives, several analyses were carried out. The ANOVA and Chi-square approach are employed for demographic analysis in order to discover statistically significant differences and whether a correlation between demography and fake news awareness exists. Cronbach’s alpha is used to gauge reliability. Pearson correaction analysis is performed to determine each variable’s impact on the effectiveness of the toolkit being employed.

5. IMPLEMENTATION

The overall implementation of the suggested approach is described in this section along with specific toolkit demonstrations. The overall layout of the web application used to implement the toolkit and survey questionnaire tools. Figure 3 shows the process of the implementation of the toolkit. The description of tools used, the respondent’s selection, time allocation, toolkit implementation are provided. These descriptions are shown in section 5.1 to section 5.5.

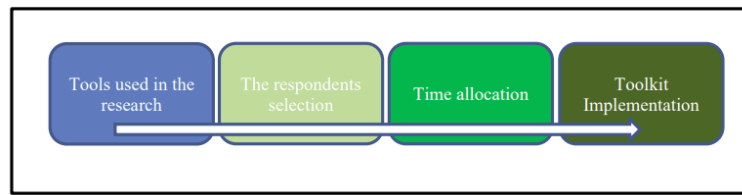


Figure 3. Process on the implementation of toolkit

5.1. Tools used

Google Form and Wix.com are the tools that were employed in this research study. The survey was created and made public using Google Form. Because it saves money and time, Google form is used to conduct the survey. Additionally, the survey and quiz replies are already in the Google Form spreadsheet, making data collection and analysis easier.

5.2. The respondents selection

A sample is a collection of things, people, or things taken from a population pool for measurement. It serves as a subgroup of the population under research with traits in common [41]. In order to gather information from them and generalise the research's conclusions, the population from the sample is used. The study needs to define the study population. The sample size is equally crucial.

5.3. Time allocation

Pre-survey, toolkit completion, and post-survey each take about 20 to 30 minutes per person to complete. The data collection period was 11 days, from August 20, 2019, to August 30, 2019, and the appropriate time was selected. Each of the three surveys-the pre-survey, toolkit completion, and post-survey-takes a person 20 to 30 minutes to complete. The right time was chosen for the data collecting, which lasted 11 days from August 20 to August 30, 2019.

5.4. Toolkit implementation

Figure 4 displays the system deployment for this application. The "fake news toolkit" application that was created was designed to be user-friendly. The toolkit's goal and additional pages that are available are displayed on the home page. Users can navigate through any section by clicking on it. First, before switching to other tabs, the user must complete a presurvey [42], [43]. The "fake news toolkit" tool was made with user-friendliness in mind. The purpose of the toolkit is made clear on the main page, along with a list of available extra pages. By clicking on any part, users can navigate through it. Before opening any additional tabs, the user must first finish a presurvey [44], [45].

5.5. Home

The fake news awareness toolkit's main menu gives users the option to jump to the home, introduction, awareness, quiz, and post survey tabs [45]. Before clicking on other tabs, the user must first complete the pre-survey. This online application has an interactive layout and a colourful background to pique users' interest.

- Survey: a questionnaire was created since it is important to understand how people understand and perceive fake news before using the toolkit. Users responded to the survey and the results and data from it were analysed.
- Introduction: the definition of fake news can be found under the introduction tab. Then, users are informed about the dangers of bogus news and why they should be cautious. Users will learn the importance of choosing the news they read carefully as a result.
- Awareness: this application included two movies on fake news to attract users' interest and inspire learners.
- Take quiz: for an effective awareness and learning application, an interactive quiz is made. This section will include 10 questions. Test your users' comprehension of the content of the web application with this quiz about fake news.
- Post survey: to assess the toolkit model's efficacy, users must complete a post-survey. In the post-survey, the same questions from the pre-survey will be asked, and the results will be recorded and analysed.

- Analysis: using the survey data, an analysis of the toolkit model's efficacy and an improvement in users' awareness will be made.

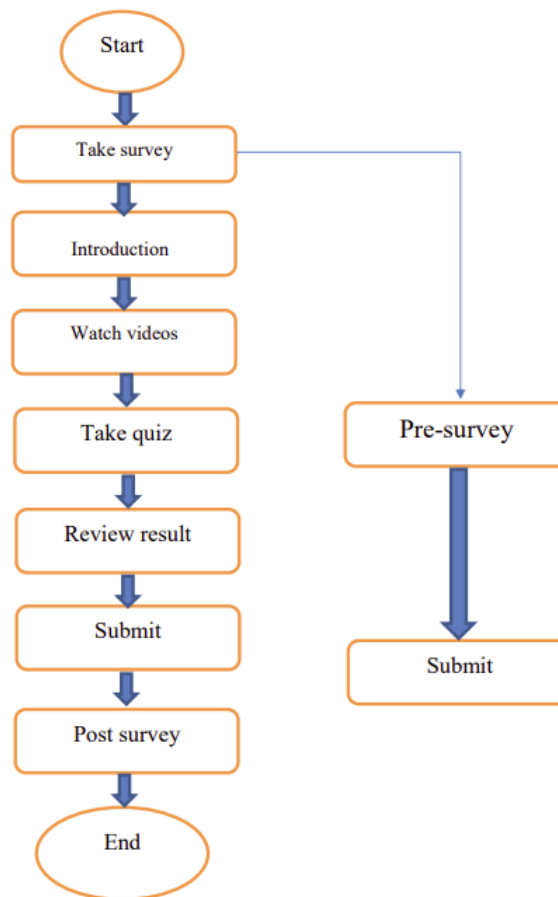


Figure 4. Flowchart of the toolkit

6. RESULTS AND ANALYSIS

This section provides the results and analysis of this paper. This paper explains the demographic participants, respondents' knowledge, respondents' behavior, and respondents' attitude are metrics to analyze the result of this paper. These metrics are explained as follows.

- Demographic participants: this poll includes six separate categories of demographic questions, including gender, age, education level, work experiences, primary news source, and social media platform [46], [47]. These inquiries are intended to determine whether these elements have an impact on the level of awareness.
- Respondents knowledge: the knowledge category consists of a total of 4 questions. The purpose of these inquiries is to gauge respondents' knowledge of fake news.
- Respondents behaviour: on behaviour, there were four questions. These inquiries are intended to learn the actual situation of the respondents. These queries centred on people's daily activities. For instance, the respondents' attitudes regarding current news sources and current events were probed.
- Respondents attitude: this portion included 11 questions to gauge respondents' knowledge of current topics relating to fake news they read and their aptitude for differentiating between actual and false information [48].

6.1. Data analysis

Reliability, often known as internal consistency, is measured using the Cronbach alpha coefficient. It is used to determine the scale's dependability, particularly for Likert questions. The alpha Cronbach's value

in this study, which is 0.380, is considered satisfactory. The elements of behaviour, attitude, and knowledge significantly influenced the potency of the fake news awareness toolkit. The elements of behaviour, attitude, and knowledge significantly influenced the potency of the fake news awareness toolkit. i) the correlation for scale one is 0.656; ii) the correlation for scale two is 0.711, and iii) the correlation for scale two is 0.632.

All connections were noteworthy. The hypothesis that there is a positive correlation between media literacy and fake news awareness level and rejects the null hypothesis that there is no correlation between media literacy and fake news awareness level [49]-[51]. A one-sample T-test is used to determine whether there is a significant difference between the population mean and the hypothesised value. The null hypothesis was rejected because there is a significant difference that is less than 0.05. $N-1$ ($110-1=109$) is the value of the estimated T divided by the value of the degree of freedom.

6.2. Discussion

The demographic analysis was performed using SPSS data analysis. The investigation revealed that gender, age, the main news source, and the social media platform used had no bearing on awareness. However, a demographic study of the responses revealed that those with prior work experience had a higher awareness level than those without. This is connected to their organization's workplace culture, which consistently emphasises the value of awareness.

Respondents with a bachelor's degree or higher were more informed than those with less education. This is related to the first demographic analysis since respondents with a bachelor's degree or higher were more likely to have prior work experience. They had a greater knowledge of bogus news and were more concerned about it. The association between media literacy or knowledge and awareness was demonstrated through Pearson correlation. The first hypothesis, "Increasing media literacy has an impact on increasing the level of false news awareness," was validated by these findings. The second claim is that the fake news toolkit significantly raises people's awareness of it.

7. CONCLUSION

This study's fake news toolkit is a tool that has the potential to enhance and have an impact on respondents' understanding of, propensity towards, and awareness of false news. In order to meet the research objectives, factors that affect each question area (media knowledge, behavior, awareness, and opinion) on the degree of fake news awareness were examined. There were two research hypotheses put out (H1: increasing media literacy has an effect on raising false news awareness. Knowledge has an impact on the whole scale (0.656). The hypothesis has been supported by this connection. H2: the fake news toolkit has a major influence on raising people's awareness of fake news. The overall scale has been impacted by attitude (0.711), which is more than the total measure that supported the H2. 110 respondents were gathered for the pre-and post-surveys, which were done in a manufacturing company and a local institution because anyone could become a victim of false information. In order to answer the research questions, achieve the study objective, and validate the analysis's justification, several surveys were conducted.

8. RECOMMENDATIONS AND FUTURE WORK

Below are some suggestions for this study based on the conclusion: i) survey a larger population to obtain more thorough information from the sample; and ii) the toolkit needs to be enhanced into a more organised format for training or seminars with information covering fake news introduction, awareness, and other related subjects. For instance, incorporating this subject into the curriculum.

REFERENCES




- [1] E. C. Tandoc, Z. W. Lim, and R. Ling, "Defining 'fake news,'" *Digital Journalism*, vol. 6, no. 2, pp. 137–153, Feb. 2018, doi: 10.1080/21670811.2017.1360143.
- [2] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 30, no. 2, pp. 778–786, May 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.
- [3] R. K. Kripakrishna and K. A. Clara, "An awareness about phishing attack and fake news using machine learning technique," in *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Apr. 2022, pp. 1–5, doi: 10.1109/ICDCECE53908.2022.9793225.

- [4] J. Baptista and A. Gradim, "A working definition of fake news," *Encyclopedia*, vol. 2, no. 1, pp. 632–645, Mar. 2022, doi: 10.3390/encyclopedia2010043.
- [5] H. Allcott and M. Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives*, vol. 31, no. 2, pp. 211–236, May 2017, doi: 10.1257/jep.31.2.211.
- [6] S. A. John and P. Keikhosrokiani, "COVID-19 fake news analytics from social media using topic modeling and clustering," in *Big Data Analytics for Healthcare*, Elsevier, 2022, pp. 221–232.
- [7] M. A. Al-Shareeda, S. Manickam, and S. A. Sari, "A survey of SQL injection attacks, their methods, and prevention techniques," in *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)*, Nov. 2022, pp. 31–35, doi: 10.1109/ICDSIC56987.2022.10075706.
- [8] Y. U. Chandra, Surjandy, and Ernawaty, "Higher education student behaviors in spreading fake news on social media: a case of LINE group," in *2017 International Conference on Information Management and Technology (ICIMTech)*, Nov. 2017, pp. 54–59, doi: 10.1109/ICIMTech.2017.8273511.
- [9] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-fog: a novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, Mar. 2023, doi: 10.3390/math11061446.
- [10] J. Wang, S. Makowski, A. Cieslik, L. Haibin, and L. Zhihan, "Fake news in virtual community, virtual society, and metaverse: a survey," *IEEE Transactions on Computational Social Systems*, pp. 1–15, 2023, doi: 10.1109/TCSS.2022.3220420.
- [11] C. Melchior and M. Oliveira, "Health-related fake news on social media platforms: a systematic literature review," *New Media & Society*, vol. 24, no. 6, pp. 1500–1522, Jun. 2022, doi: 10.1177/14614448211038762.
- [12] M. Azzimonti and M. Fernandes, "Social media networks, fake news, and polarization," *European Journal of Political Economy*, vol. 76, p. 102256, Jan. 2023, doi: 10.1016/j.ejpoleco.2022.102256.
- [13] B. A. Mohammed *et al.*, "FC-PA: fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023, doi: 10.1109/ACCESS.2023.3247222.
- [14] G. D. Domenico, J. Sit, A. Ishizaka, and D. Nunan, "Fake news, social media and marketing: a systematic review," *Journal of Business Research*, vol. 124, pp. 329–341, Jan. 2021, doi: 10.1016/j.jbusres.2020.11.037.
- [15] N. Alnazzawi, N. Alsaedi, F. Alharbi, and N. Alaswad, "Using social media to detect fake news information related to product marketing: the fakeads corpus," *Data*, vol. 7, no. 4, p. 44, Apr. 2022, doi: 10.3390/data7040044.
- [16] Z. G. Al-Mekhlafi *et al.*, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, p. 872, Feb. 2023, doi: 10.3390/electronics12040872.
- [17] A. Bani-Hani, O. Adedugbe, E. Benkhelifa, and M. Majdalawieh, "Fandet semantic model: an owl ontology for context-based fake news detection on social media," in *Combating Fake News with Computational Intelligence Techniques. Studies in Computational Intelligence*, Cham: Springer, 2022, pp. 91–125.
- [18] O. D. Apuke and B. Omar, "Fake news and COVID-19: modelling the predictors of fake news sharing among social media users," *Telematics and Informatics*, vol. 56, p. 101475, Jan. 2021, doi: 10.1016/j.tele.2020.101475.
- [19] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.
- [20] M. T. M. Máñez, A. M. Cano, and F. Díez, "Impact of fake news on social networks during COVID-19 pandemic in Spain," *Young Consumers*, Mar. 2023, doi: 10.1108/YC-04-2022-1514.
- [21] X. Li, P. Lu, L. Hu, X. Wang, and L. Lu, "A novel self-learning semi-supervised deep learning network to detect fake news on social media," *Multimedia Tools and Applications*, vol. 81, no. 14, pp. 19341–19349, Jun. 2022, doi: 10.1007/s11042-021-11065-x
- [22] Surjandy, H. Alianto, and Y. U. Chandra, "The smartphone for disseminating of fake news by the university students game player," in *2017 International Conference on Information Management and Technology (ICIMTech)*, Nov. 2017, pp. 14–18, doi: 10.1109/ICIMTech.2017.8273503.
- [23] A. Baharum *et al.*, "Biodiversity awareness using mobile application: Ikimono Mikke," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2017, pp. 334–339, doi: 10.1109/ICTC.2017.8190998.
- [24] Y. Peker, L. Ray, and S. Silva, "Online cybersecurity awareness modules for college and high school students," in *2018 National Cyber Summit (NCS)*, Jun. 2018, pp. 24–33, doi: 10.1109/NCS.2018.00009.
- [25] A. Campan, A. Cuzzocrea, and T. M. Truta, "Fighting fake news spread in online social networks: actual trends and future research directions," in *2017 IEEE International Conference on Big Data (Big Data)*, Dec. 2017, pp. 4453–4457, doi: 10.1109/Big-Data.2017.8258484.
- [26] N. Ahmed, U. Kulsum, I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: an analysis from Bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dec. 2017, pp. 788–791, doi: 10.1109/R10-HTC.2017.8289074.
- [27] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "Intelligent drone-based IoT technology for smart agriculture system," in *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)*, Nov. 2022, pp. 41–45, doi: 10.1109/ICDSIC56987.2022.10076170.
- [28] Y. Wang, L. Wang, Y. Yang, and Y. Zhang, "Detecting fake news by enhanced text representation with multi-EDU-structure awareness," *Expert Systems with Applications*, vol. 206, p. 117781, Nov. 2022, doi: 10.1016/j.eswa.2022.117781.
- [29] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 1, p. 518, Jan. 2022, doi: 10.11591/ijeecs.v29.i1.pp518-526.
- [30] A. Gelfert, "Fake news: a definition," *Informal Logic*, vol. 38, no. 1, pp. 84–117, Mar. 2018, doi: 10.22329/il.v38i1.5068.
- [31] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, Jan. 2023, doi: 10.3390/math11020399.
- [32] A. C. Charles and J. D. O. Sampaio, "Checking fake news on web browsers: An approach using collaborative datasets," in *CEUR Workshop Proceedings*, 2018, vol. 2247.




- [33] O. D. Apuke, B. Omar, and E. A. Tunca, "Effect of fake news awareness as an intervention strategy for motivating news verification behaviour among social media users in nigeria: a quasi-experimental research," *Journal of Asian and African Studies*, p. 002190962210793, Feb. 2022, doi: 10.1177/00219096221079320.
- [34] A. T. Wibowo, "Hoax and fake news by saracen syndicate and the problems for national cyber security," *Indonesian Journal of Counter Terrorism and National Security*, vol. 1, no. 1, pp. 91–108, Jan. 2022, doi: 10.15294/ijctns.v1i1.56732.
- [35] C. Sinclair, "Parody: fake news, regeneration and education," *Postdigital Science and Education*, vol. 2, no. 1, pp. 61–77, Jan. 2020, doi: 10.1007/s42438-019-00054-x..
- [36] V. L. Muzykant, M. A. Muqith, R. R. Pratomo, and V. Barabash, "Fake news on COVID-19 in Indonesia," in *Pandemic Communication and Resilience. Risk, Systems and Decisions*, Cham: Springer, 2021, pp. 363–378.
- [37] M. R. Nelson and J. Park, "Publicity as covert marketing? the role of persuasion knowledge and ethical perceptions on beliefs and credibility in a video news release story," *Journal of Business Ethics*, vol. 130, no. 2, pp. 327–341, 2015.
- [38] B. McNair, *Fake news: falsehood, fabrication and fantasy in journalism*. Routledge, 2017.
- [39] Z. G. Al-Mekhlafi *et al.*, "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, Mar. 2023, doi: 10.3390/s23073543.
- [40] J. Golbeck *et al.*, "Fake news vs satire: a dataset and analysis," in *WebSci 2018 - Proceedings of the 10th ACM Conference on Web Science*, May 2018, pp. 17–21, doi: 10.1145/3201064.3201100.
- [41] B. S. Reddy and A. P. S. Kumar, "Multimodal approaches based on fake news detection," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Feb. 2023, pp. 751–755, doi: 10.1109/ICAIS56108.2023.10073839.
- [42] M. R. H. Shezan, M. N. Zawad, Y. A. Shahed, and S. Ripon, "Bangla fake news detection using hybrid deep learning models," in *Applied Informatics for Industry 4.0*, 2023, pp. 46–60.
- [43] K. Srinivasa and P. S. Thilagam, "Multi-layer perceptron based fake news classification using knowledge base triples," *Applied Intelligence*, vol. 53, no. 6, pp. 6276–6287, Mar. 2023, doi: 10.1007/s10489-022-03627-9.
- [44] S. DeJong, "Playing with fake news: state of fake news video games," *International Journal of Games and Social Impact*, vol. 1, no. 1, pp. 94–111, Jan. 2013, doi: 10.24140/ijgsi.v1.n1.05.
- [45] M. I. Nadeem *et al.*, "HyproBert: a fake news detection model based on deep hypercontext," *Symmetry*, vol. 15, no. 2, p. 296, Jan. 2023, doi: 10.3390/sym15020296.
- [46] C. Lees, "Fake news: the global silencer: the term has become a useful weapon in the dictator's toolkit against the media. Just look at the Philippines," *Index on Censorship*, vol. 47, no. 1, pp. 88–91, Apr. 2018, doi: 10.1177/0306422018769578.
- [47] N. Pyrhönen and G. Bauvois, "Conspiracies beyond fake news. producing reinformation on presidential elections in the transnational hybrid media system," *Sociological Inquiry*, vol. 90, no. 4, pp. 705–731, Nov. 2020, doi: 10.1111/soin.12339.
- [48] T. B. Fischer, "Editorial: IA, alternative facts and fake news – Is the post-factual turn starting to turn?," *Impact Assessment and Project Appraisal*, vol. 36, no. 2, pp. 129–130, Mar. 2018, doi: 10.1080/14615517.2018.1426846.
- [49] S. Jayakumar, B. Ang, and N. D. Anwar, "Fake news and disinformation: Singapore perspectives," in *Disinformation and Fake News*, Singapore: Springer, 2021, pp. 137–158.
- [50] P. Choudhary, S. Pandey, S. Tripathi, and S. Chaurasiya, "Fake news detection based on machine learning," in *Advances in Smart Communication and Imaging Systems. Lecture Notes in Electrical Engineering*, Singapore: Springer, 2021, pp. 67–75.
- [51] G. Belova and G. Georgieva, "Fake news as a threat to national security," *International conference KNOWLEDGE-BASED ORGANIZATION*, vol. 24, no. 1, pp. 19–22, Jun. 2018, doi: 10.1515/kbo-2018-0002.

BIOGRAPHIES OF AUTHORS







Mahmood A. Al-Shareeda    obtained his Ph.D. in advanced computer network from University Sains Malaysia (USM). He is currently a postdoctoral fellowship at National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security. He can be contacted at email: alshareeda022@usm.my.







Murtaja Ali Saare    is an assistant professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master's degree in information technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph.D. at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work in reputable indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sauc.edu.iq.



Selvakumar Manickam     is currently working as an associate professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, internet of things, industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.



Shankar Karuppayah     is received the B.Sc. degree (Hons.) in computer science from Universiti Sains Malaysia, in 2009, the M.Sc. degree in software systems engineering from the King Mongkut's University of Technology North Bangkok (KMUTNB), in 2011, and the Ph.D. degree from TU Darmstadt with his dissertation titled advanced monitoring in P2P Botnets, in 2016. He has been a senior researcher/a postdoctoral researcher with the Telecooperation Group, TU Darmstadt, since July 2019. He has also been a senior lecturer at the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, since 2016. He is currently working actively on several cybersecurity projects and working groups, e.g., the National Research Center for Applied Cybersecurity (ATHENE), formerly known as the Center for Research in Security and Privacy (CRISP). He can be contacted at email: kshankar@usm.my.