Policies and Platforms for Fake News Filtering on Cybercrime in Smart City Using Artificial Intelligence and Blockchain Technology

Assoc.Prof.Dr.Pannee Suanpang[1*]
Suan Dusit University, Thailand

Pattanapong Pothipasa[2]
Sisaket Rajabhat University, Thailand, ppothi168@gmail.com

Asst.Prof.Dr.Titiya Netwrong[3]
Suan Dusit University, Thailand

Abstract
In this era of technological disruption, as city dwellers change into smart city inhabitants, the perception of information via digital channels is becoming more prevalent and used for decision-making and lifestyle choices. However, the perception of fake news or social media has resulted in poor decision-making and anxiety among smart city residents. Recognizing the importance of filtering false information for the smart city population, this research proposed a policy and platform for filtering false information to be presented to the citizens of Sisaket Smart City, Thailand; this was to ensure the efficient and secure use of large amounts of citizens' information, as well as information exchange between agencies. Additionally, the study was designed to kick-start the use of information in a smart city to make it more efficient and capable of filtering out material that could have harmful consequences or fake news. Recognizing its significance, the researchers proposed building regulations and platforms for detecting and filtering fake news in smart cities using artificial intelligence and blockchain technology. The findings indicated that urban inhabitants who moved into Thailand's smart cities, such as Sisaket, were highly receptive to the employment of rules and platforms to filter fake news.

Keywords: Fake News Filtering, Policies, Smart City Platform, Artificial Intelligence, Blockchain Technology

[1] Department of Information Technology, Faculty of Science & Technology, Suan Dusit University, Thailand, pannee_sua@dusit.ac.th
[2] Faculty of Liberal Arts and Sciences, Sisaket Rajabhat University, Thailand, ppothi168@gmail.com
[3] Department of Information Technology, Faculty of Science & Technology, Suan Dusit University, Thailand, titiya_net@dusit.ac.th

Introduction

The emergence of the World Wide Web and the quick adoption of social media platforms such as Facebook and Twitter have resulted in an unprecedented amount of knowledge being distributed across human history (Pannee Suanpang & Pitchaya Jamjuntr, 2021; P. Suanpang et al., 2022). With the increased usage of social media, consumers create and share more information than ever before (Jermsittiparsert, 2019), some of which are inaccurate and unrelated (P Suanpang & P Jamjuntr, 2021). Classifying text articles automatically for inaccuracy or misinformation is a complex undertaking. Even professionals in a given field must consider various factors before judging an article's validity (P Suanpang et al., 2021).

False news is information that is provided as news to mislead the public. To harm the agency's legal entity or individual, acquire financial benefit, or exert political influence. Fake news makers frequently employ sexy, deceptive, or entirely false headlines to enhance their readership, online sharing, and revenue from internet clicks. Similar to the "clickbait" headline, online is sexual and financially dependent on advertising money regardless of whether the printed material is truthful or not (Ahmad et al., 2020; P. Suanpang et al., 2022). Apart from economic motivations, the creation and dissemination of fake news may be systematic political operations involving manipulative techniques or psychological persuasion or the creation of conspiracy theories to confuse information consumers or cast doubt on facts or evidence (Ahmad et al., 2020). Numerous factors contribute to the propagation of fake news these days, including producing material for advertising businesses and simple access to cash via online advertising. Political divisions are a growing trend that fights attention with the correct news topics.

Additionally, fake news substantially affects media coverage and makes it more difficult for journalists to create essential news by undermining news consumers' credibility through widespread dissemination of fake news (Aphiwongsophon & Chongstitvatana, 2018; P. Suanpang et al., 2022). Fake news has a detrimental effect on individuals and society because it purposefully persuades consumers to accept widespread misunderstandings to further a particular agenda (Talwar et al., 2020). This idea is backed up by extensive research that demonstrates that individuals overestimate the effects of socially harmful content such as gambling, pornography, and alcohol advertising to others (Rojas et al., 1996).

Fake news is a form of cybercrime or computer crime, which is defined as the use of a computer or other electronic device connected to the Internet to damage, change, or steal information for personal advantage (Ahmad et al., 2020; Aldwairi & Alwahedi, 2018; P. Suanpang et al., 2022). This may result in both direct and indirect damage to the organization, company, or individual involved, for example, by hacking into the victim's computer operating system via email by sending e-mails and attaching malware files (Malware) and writing an e-mail inviting the victim to open the file, or by attacking corporate database systems with ransomware (Ransomware) to demand payment (Leukfeldt & Holt, 2022). In an era where people have increased access to communication technology and digital information obtained through various social media transactions or even the Internet of Things (IoT), devices are used for decision-making and day-to-day activities. Thus, at the moment, it is an issue that has drawn the attention of well-wishers and has switched from traditional criminal activity to online harassment and attacks (Yeboah-Ofori et al., 2021).

Case studies of fake news and cybercrime that are occurring and harming people worldwide, particularly in smart cities. For example, an examination into the 2013 US terrorist bombing at the Boston Marathon discovered that word about the attack

disseminated rapidly via social media and other multimedia platforms. The incident illustrated how social media and other multimedia platforms significantly aided the public in providing information about suspects, including essential facts and incentives (Elmaghraby & Losavio, 2014). This swiftly resulted in the suspect's arrest. However, the news sent by these channels also contributes to the accusers' deception and unjust conduct. The ramifications of this episode beg the following question: Can we rely on information from these sources without receiving training? State security services should be responsible for the appropriate use of these data to examine and assess telecommunications legislation and transaction data. This case demonstrates that this occurrence is beyond the scope of the US National Security Agency's proper mission. One could argue that the benefits of social media information exceed the risks when used responsibly and following a democratic society's rights and freedoms (Elmaghraby & Losavio, 2014).

Simultaneously, in Thailand's Sisaket province, residents are beginning to change into a "smart city" population as a result of information gleaned from the social media globe. Following the necessary authority and mission of the local government for the operation of the Sisaket Municipality, the adoption of modern digital technology is the primary force for development. This would establish a link in line with Thailand's national development strategy, which is guided by the motto "Stability, Prosperity, Sustainability," the 20-year National Strategy Framework (2018-2037), the Twelfth National Economic and Social Development Plan (2017-2021), and the Thailand 4.0 policy. Sisaket Municipality has established the Sisaket Smart City Project management to develop concrete and successful plans, policies, and practices. To prepare a plan for the development of Sisaket's smart city, two committees were established; additionally, an ad hoc committee on intelligent citizens, a working group on intelligent environment, and a working group on government intelligence administration were established (Proposal for receiving smart city consideration, revised June 2021).

According to the situation review conducted in the research area, the population had been heavily influenced by fake news about the COVID-19 outbreak in numerous areas, including the side effects of the COVID-19 vaccines, resulting in cases of injury to the health system in the smart city, with residents fearful of dying after receiving the vaccine. As a result of the effect of fake news on people's decision-making and refusal to undergo vaccine injections, COVID 19 can spread throughout the city, causing harm to the national health system, economy, and people's quality of life (Pattaya Mail, 2021).

As a result of this situation, the local administration of Sisaket province developed a surveillance system for locations where COVID-19 is spreading or where people are traveling to get vaccinated at a government-provided location (Okereafor, 2021). However, most Sisaket residents are low- to middle-income and tend to believe news shared on social media platforms such as Facebook, Line, and Twitter, despite their occasional lack of information. This problem arises due to fake news about the Covid-19 outbreak in Sisaket province, which significantly influences the economy and mental health of the population in Sisaket smart city.

To combat fake news and cybercrime on the social media platforms used by residents of Sisaket smart city, establishing a clear public policy that considers online news is critical for filtering out the news that may qualify as fake news and other cyber threats from spreading to residents of Sisaket smart city. In compliance with the competent authorities and the Sisaket Municipality's objective to enhance local development guidelines and public services. Additionally, when filtering material on such social networks, adopting classic

algorithms may help avoid issues associated with cyber criminals' evolving assault techniques (Leukfeldt & Holt, 2022). As a result, a more practical solution is to employ artificial intelligence to identify patterns in data or attacks that may represent fraudulent news or crimes (Aphiwongsophon & Chongstitvatana, 2018). Additionally, to incorporate artificial intelligence into detecting fake news patterns and the cybercrime mentioned above attacks. Verifying whether the source or owner of the news is credible or not is possible through the use of blockchain techniques such as Proof-of-Authority protocols, which are a type of blockchain technology that can trace back to see if a transaction was confirmed, who confirmed it, and whether it was confirmed in good faith or not (Kolluri & Murthy, 2021). If the transaction is traced back and fraud or error is discovered, the person who confirmed the transaction may lose reputation (Chen et al., 2020). These cybercrimes wreak havoc on people's mental health and disrupt daily life. Recognizing the necessity for such monitoring and banning of fake news, this research spurred the development of a paradigm and platform that utilized artificial intelligence and blockchain-related technologies to automatically categorize and filter news articles for smart city people (Kolluri & Murthy, 2021).

The condition of cybercrime and fake news in smart cities prompted research intending to develop regulations and platforms for the filtering of fake news related to cybercrime through the use of artificial intelligence and blockchain technology.

Literature review

Smart City

The term 'smart city' first appeared between 1986 and 1990 in the literature on innovative urban development and publications on Japanese Technopolis projects such as Lipman et al. (1986), and Masser (1990), (Batty, 1990), where it is defined as the use of information technology and networks to sustain technological development and a city's competitive advantage. Simultaneously, the phrase "smart city" was used to refer to urban innovation. These initiatives emphasize sustainable mobility through information technology, information technology, and communication to deliver municipal services and improve cities' performance in socioeconomic environments (Ajah et al., 2020; Hall, 2014; Wemmerlöv, 1990).

On the other hand, a smart city is defined by innovation, information technology, and virtual cities. The term "smart city" focuses on innovation and information technology while still having physical qualities, a complex social fabric, and digital infrastructure. With an emphasis on electronic governance and virtual presentations (Besselaar & Koizumi, 2005; Ishida & Isbister, 2000), there is an abundance of literature discussing the concept of smart digital engagement technology. For urban development and planning in the twenty-first century, digital cyber information exchange and knowledge and innovation systems are critical. This paper highlights an approach to transforming cities: describes a series of innovations in sustainable urbanization by broadband networks, sensors, information management technologies, and innovative systems for urban development and planning in the 21st-century application software and electronic services. Additionally, both the city and innovation systems are transforming due to these technologies, end-users, and other organizations. Innovative behavioral patterns can be more easily created.

The growing trend of smart city populations necessitates the development of structures, employment, and urban environmental management to accommodate the growing population (Mitchell) effectively. Every group in society must enjoy a high standard of living, a healthy environment, a sound economy, sound management, and technological

advancements by developing a smart city that leverages modernity and intelligence. Technology and innovation (Besselaar & Koizumi, 2005; Ishida & Isbister, 2000) can be achieved by improving urban management in areas such as economic development, conservation, and environmental rehabilitation, and livelihoods, as well as urban management according to prefectural and national strategic urbanization plans, to reduce society's ignorance in all dimensions (Rygielska, 2020; Salavrakos, 2020; Schreuders et al., 2020; Sisaket Municipality, 2021).

Policy & Platform for Fake News

While faith in government is not a passive theoretical concept, it significantly impacts public health during the COVID-19 crisis. It is necessary to have a thorough scholarly grasp of the potency and attractiveness of fake news. According to Porumbescu (2018), the evolution of online media has nothing to do with public perceptions of government; however, with the discussion of fake news as "The Deep States" and growing political polarization as a result of rising levels of global digital inclusion, it has become increasingly difficult to contain the spread of misinformation. Social media platform activities (hereafter referred to as SMP) and the government have targeted sources of misinformation. However, individual user participation with fake news (sharing and boosting links) adds another dimension to the problem. The fake news problem can be handled by analyzing the motives that motivate individuals to participate in fake news.Hartley and Vu (2020) provide a mathematical approach for calculating the cost of an individual making low- or high-level efforts to combat fake news. Its objective is to expose techniques via which SMPs and governments can intervene on an individual and broad-scale to prohibit the intentional transmission of misleading information. This article discusses the research on fake news on social media and government policy initiatives to combat it. This was followed by a description of the model, with subsequent sections focused on policy implications and recommendations for connecting model discovery to performance. Conclusions have a broader influence on the occurrence. It is 'behind the truth' in policy formulation and necessitates continued research on race epistemology.

Cybercrime

Cybercrime or cybercrime is a social problem very similar to traditional crime in that it takes on a multitude of forms to express or benefit the perpetrator (Leukfeldt & Holt, 2022). Harassment of others' rights via online channels and cyberbullying can provide offenders with a sense of authority comparable to that seen in real-world violence (Holt & Bossler, 2015). Phishing is the most prevalent type of cyber fraud, as it exposes consumers to personal information that can be utilized for financial benefit. Additionally, hackers have some similarities with real-world criminals, which may confuse the nature of the expertise or versatility discovered in real-world crime research. For instance, a person may employ computer hacking techniques to obtain access to a computer network to steal files or other sensitive information that could be used to deceive or sell to others. The same can be done with malicious software, although not all hackers employ these techniques. Although these acts are not identical, they might be clubbed together; this can be misleading when attempting to quantify their involvement in cybercrime in general. An empirical study on cybercrime has centered on determining the nature of cybercrime's specialization or adaptability. Most quantitative studies have concentrated on the prevalence of fault types in the collegiate population. This has concentrated on simple forms of harassment that may yield marginal economic gains (Holt & Bossler, 2015; Maimon & Louderback, 2019).

Fake news is a type of cybercrime that refers to inaccurate information, misleading information, or whose source cannot be verified (Ahmad et al., 2020). This article may have been made to discredit, defraud, or attract attention. At the moment, the many varieties of fake news can be classified as follows: (1) lick bet fake news: this form of fake news frequently includes visually appealing content to entice viewers at the expense of the facts. (2) Satire/parody fake news: fake news with this type of material is intended to be amusing and entertaining. The information is entertaining, but some readers may understand it is accurate. (3) Propaganda of the fake news variety: this content is deceptive and persuasive to the reader. (4) Skewed/hyperpartisan false news: This content is frequently biased while claiming to be objective. (5) News that unreliable journalists may write without verifying their sources or conducting extensive self-examination of the facts.

Artificial Intelligent for Filter Fake News

Support Vector Machine (SVM): This is a model for binary classification problems that can be used in various ways. The SVM model's objective is to estimate the hyperplane (or decision boundaries) from the properties defined to categorize the data points and the hyperplane's size changes (Ahmad et al., 2020). There are numerous options for a hyperplane in an N-dimensional space, depending on the number of features. The objective would be to determine the lane that divides the data points of the two classes by the margin's most significant value Aphiwongsophon and Chongstitvatana (2018) pioneered the use of SVM to detect false news, and in this work, the researchers compared SVM to ELM in detecting fake news.

Extreme Learning Machine: Machine learning techniques are used to classify queries based on their lexical properties, which need a high level of processing power and complicated data structures because the terms may be unique (or high dimensions). Thus, by focusing on semantic features, the dimension of the feature space can be significantly reduced. The researchers chose the Extreme Learning Machine (ELM) to construct a platform comparable to Hardy and Cheah (2013), which employed an ELM to categorise semantic attribute questions in order to increase both training and testing speeds when compared to the SVM benchmark. Additionally, the prefix extraction and lexical disambiguation algorithms have been optimised. These improvements resulted in a 0.2% gain in accuracy for coarse classifications when compared to the benchmarks. As a result, accuracy was reduced by 1.0 percent, however this was offset by a significant gain in speed (average of 92.1 percent).

Blockchain Technology for Filter Fake News

IPFS: Is a peer-to-peer file-sharing technology that has grown in popularity due to Distributed Hash Tables (DHT). Additionally, IPFS employs a unique hash of 46 bytes for each image or video, which allows for size reduction during access and storage. In distributed hash, the IPFS hash is also resolved. Each time a grid is changed using the original photo or video frame due to research transactions (Kumar et al., 2021). This uniquely identifies each image or video published on a blockchain network's IPFS distributed file-sharing system. The researchers chose the IPFS file system over the Internet 2.0 file system to create a highly efficient and secure computing platform and enable distributed computing in the blockchain era.

Proof of Authority (PoA): A consensus mechanism relies on a node called an Authority or Validator to verify transactions within the blockchain network. In this case, the Authority node is not required to wait and verify the transaction. This merely installs software to verify POA transactions. The owner of this type of node is required to publicly disclose their identity (Chen et al., 2020). PoA protocols that prevent splits are the most integrated and commonly-used variants of Ethereum, parity, and get and are currently in use worldwide. PoA gained rapid popularity and is now available as a software-as-a-service (SaaS). Additionally, service providers provide this protocol, and it is used in various blockchain networks; nevertheless, to the researchers' knowledge, the PoA protocol's level of security has not been adequately assessed.

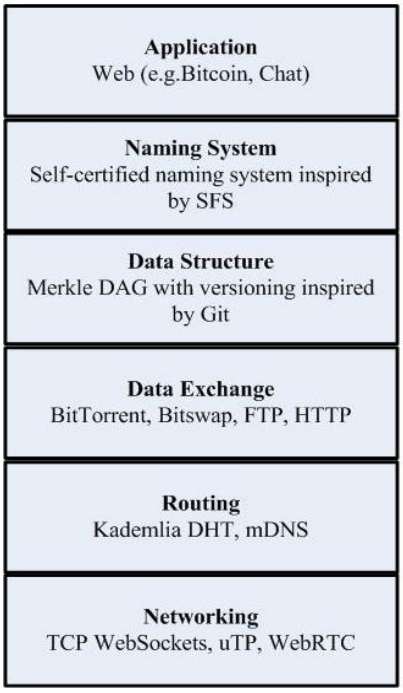

Figure 1: IPFS Stacks

Research Methodology

To Develop A Strategy And Platform For Screening Fake News For The Residents Of Sisaket's Smart City, The Researchers Followed The Following Steps: (1) Researched The Subject, (2) Designed The System's Architecture (Figure 2), (3) Developed The Platform, (4) Collected Data From Social Networks To Create Ai Training Models, (5) Conducted Machine Learning Training, (6) Attempted To Predict The Percentage Of Fake News From Interesting Sources, And (7) Drafted A Satisfaction Survey For System Users.

This Research Begins With Establishing Policies And A Platform For Phony New Filters (Figure 2). The Hypothesis In This Study Is Based On A Review Of The Literature On Avoiding Fake News From Negatively Affecting The Inhabitants Of Sisaket Smart City. We Have Identified A Research Hypothesis That Government Policymaking And Platforms Based On Artificial Intelligence And Blockchain Technology That Verify The Identity And Rights Of Information Owners To Filter And Alert On Fake News Will Significantly Reduce The Negative Impact On People In Sisaket's Smart City. The Researchers Created The System Architecture Depicted In Figure 3 To Use It To Test The Hypothesis Mentioned Above As A Data-Gathering Tool.

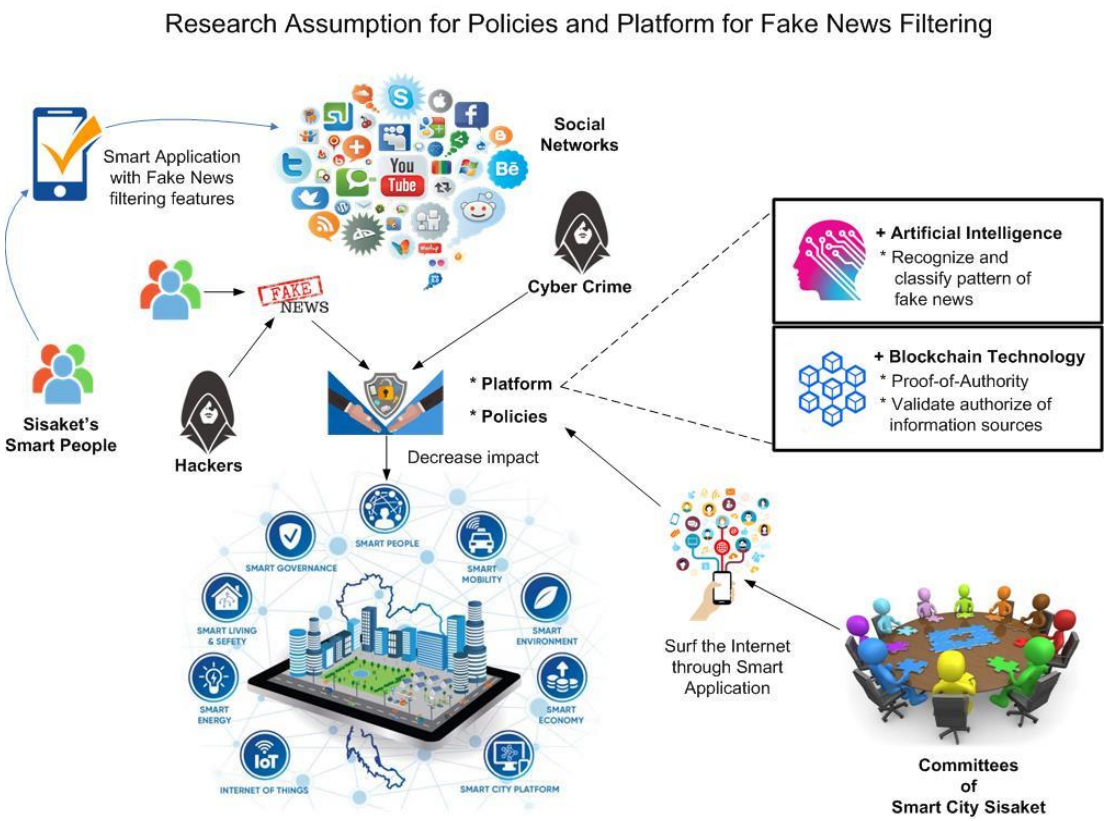

Figure 2: Research assumption for policies and platform for fake news filtering

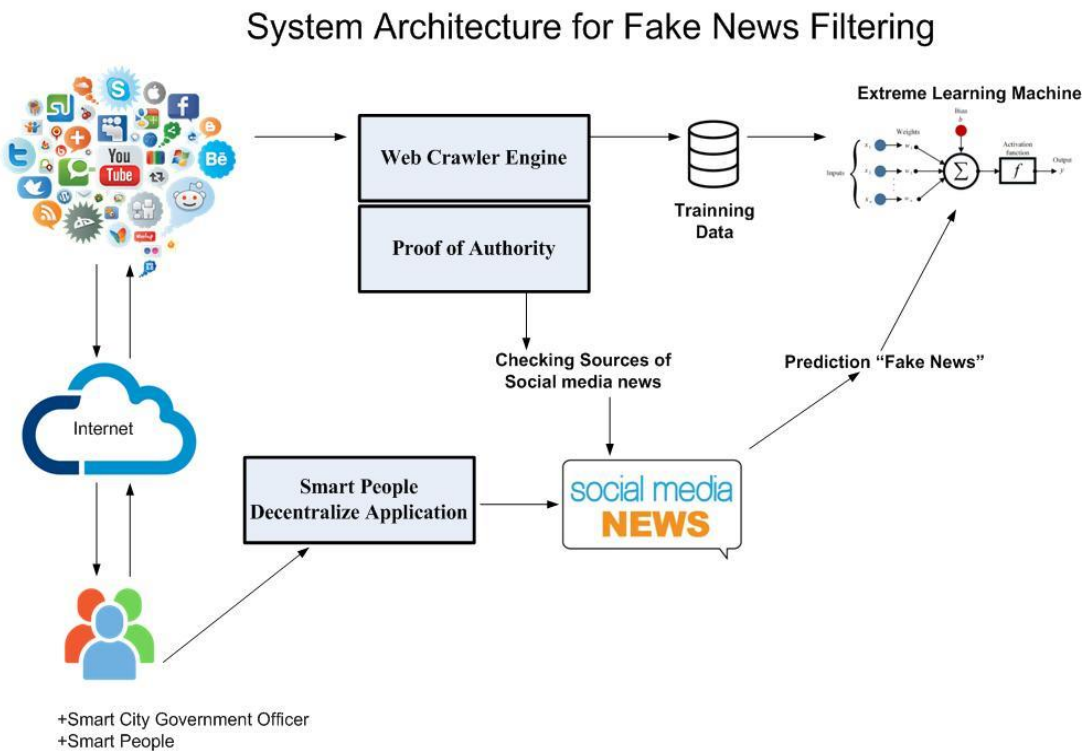

Figure 3: Theoretical framework

After completing the related research investigations, the research team met with the Sisaket Smart City Development Committee to identify a reliable information perception method for residents of the smart city in Sisaket province to inform them about the decentralized application. This would determine the similarity of social media data to fake news data, as the system or platform built employed a web crawler engine to harvest data from many sources and train it on the ELM. The study's application of machine learning algorithms to filtering fake news was compatible with Aldwairi and Alwahedi (2018) and Ahmad et al. (2020). Additionally, Sisaket City Municipality, the primary agency for news dissemination, decided to bring government information useful to the public to the IPFS network on the blockchain to facilitate the verification of the source of information and the reversibility of the source of information.

Equation 1 illustrates data from social media for clever citizens in Sisaket province from this research.

$$Information_{useful} = (Social\ Media\ News_{Fake\ Features} < Trainning\ Data) * Information_{weight}, \quad (1)$$

Where

$Information_{useful}$ stands for score of the usefulness of information
$Social\ Media\ News_{Fake\ Features}$ refers to the level of fake news attributes
$Trainning\ Data$ refers to the data obtained from the web crawler, which used to train machine learning

$Information_{weight}$ refers to the weight of information

From Equation (1), the information that would be useful to the public ($Information_{useful}$) or information that was not fake news accounted for less than 20%, which was similar to fake news in the training of machine learning ($Training\ Data$). In addition, this had a weight ($Information_{weight}$) of 1 that was traceable to the presence of an actual IPFS network and could be used by proof of authority to verify who owned the data.

Research Results

Policy & Platform for Fake News

The findings of this study indicate that Sisaket Municipality's government policy requires residents of Sisaket smart city to opt into receiving and checking news about the Covid 19 epidemic, whether it is a severe epidemic area schedule and location of vaccination services, via a fake news filtering program developed by the Sisaket smart city project advisory team. This research resulted in Sisaket Municipality implementing a concrete filtering policy for false information. For example, a smart citizen in Sisaket smart city must have internet access and the Sisaket smart city application running on a PC or smartphone, which will represent the platform in both web and mobile form. If the system discovered such information, it would bring the content on social media that people would access to compare to the pattern it had previously acquired. In this study, ELM was more sensitive to detecting similarities between fake news than SVM, which was more accurate.

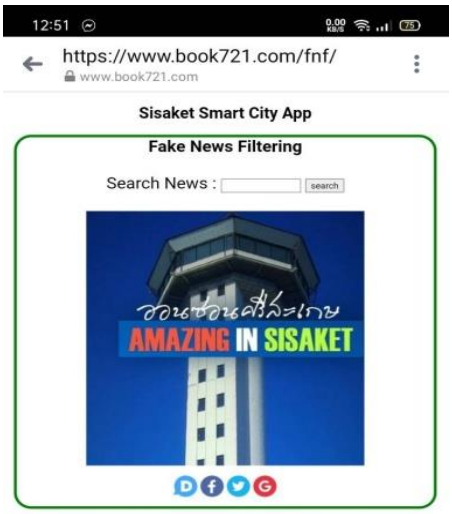

Figure 4: Fake News Filtering Service in Sisaket Smart City Application

Regarding Figure 4, once the user has entered the desired topic and pushed the search button, the user's information is delivered to the confirmation screen. When the user clicked the check button on the confirmation page, the subject and details were examined and obtained results (Figure 5).

Figure 5: Displays the confirmation screen

Regarding Figure 6, AI determined that the material was fake news after comparing the article and determining that it was from October 2020 and will be reshared. Additionally, the study team gathered the opinions of 30 residents of Sisaket province regarding their agreement with the screening of clever individuals, the platform's fraud prevention policy, and their thoughts on the platform's use.

Figure 6: Fake news analysis results

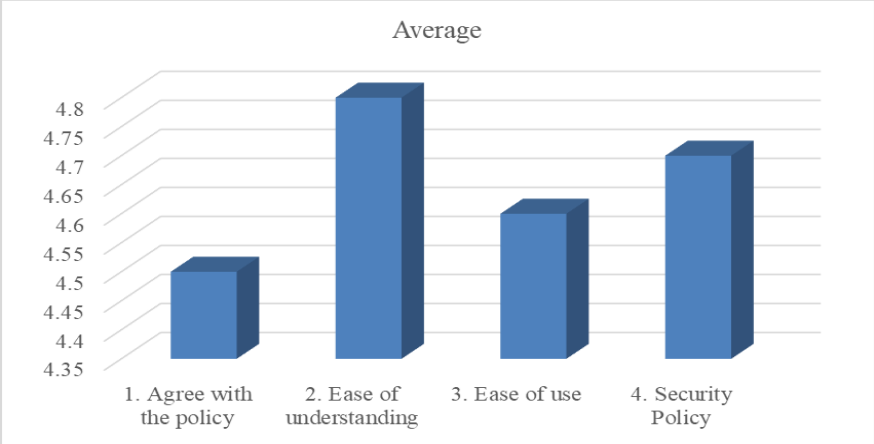

Figure 7: User Acceptance Test

Figure 7 summarises the survey findings of the policy and system evaluation in four areas: (1) agreement with the false news policy; (2) system ease of understanding; (3) system ease of use; and (4) security policy is suitable, all of which received a five-star rating (1-5). The mean of the four concerns was 4.65, indicating that the public in Sisaket smart city, policy acceptability, and the platform's responsiveness to filter misleading information, were highly reliable in this research. Additionally, this research demonstrates that the use of blockchain technology enables government officials and linked parties to trace and prove the source of information that residents of Sisaket smart city receive from social media. Because of the system's Proof-of-Authority feature, tracking births and importing data into IPFS is far easier than web 2.0's file system. When rules and platforms are used to filter material from social media that may be fake news before it reaches residents in Sisaket's smart city, It was discovered that residents of Sisaket province are content with the usage of social media information in their everyday lives, which contributes to excellent perception. Additionally, this technology lowers cybercrime in Sisaket's smart city and facilitates effective communication between the local government and the public. Finally, this enables Sisaket province's economy to grow faster than other people who lack confidence in social media information.

Discussion and Conclusion

Fake news and cybercrime are becoming severe issues that can harm the public health system and people's quality of life, particularly in smart cities. With the proliferation of fake news and cybercrime on social media and the internet, the way we use information technology and government policy should be updated. The researchers were aware of the influence and loss on the smart population in Sisaket's smart city due to exposure to fake news during this research. As a result of their investigation, the researchers advocated a policy of installing platform instances to prevent false news from entering people's computers and smartphones and detecting and blocking potential fake news data. This demonstrated that Extreme Learning Machine (ELM) was a viable alternative to Support Vector Machine (SVM) for filtering fake news, as it was faster and more accurate than SVM (SVM). The findings of this study corroborated those of (Mohawesh et al., 2021), who demonstrated that while the SVM was an intelligent algorithm for classification, it was not the ideal choice for false detection and filtering because new algorithms were still proving their proficiency in this area.

Additionally, blockchain technology is utilizing the electronic wallet system to store critical information for residents of the Sisaket smart city and transform some information into the form of NFT, which can be used to identify the owner and origin of the information. Additionally, the paradigms and workflows of the platforms offered here aided in Thailand's adoption of new smart cities. Thus, in an age where individuals rely heavily on digital information for their daily lives, they could acquire helpful knowledge and contribute to improving their quality of life. The research team intends to increase the platform's efficiency through the use of quantum computing and new blockchain technologies, such as using the electronic wallet system to collect critical information for residents of the Sisaket smart city or even converting some information into the form of NFT, which can be used to identify the owner of the information and its origin.

Acknowledgements

This work was supported by Suan Dusit University and Sisaket Rajabhat University, Thailand. In addition, the research team would like to thank the Sisaket Municipality and the Sisaket Smart City Development Committee for all their cooperation and for providing the necessary information for the research. This study is part of the research project no 65-FF-003, *"Innovation of Smart Tourism to Promote Tourism in Suphanburi Province."* Suan Dusit University funds it under the Ministry of Higher Education, Science, Research and Innovation, Thailand.

References

Ahmad, I., Yousaf, M., Yousaf, S., & Ahmad, M. O. (2020). Fake news detection using machine learning ensemble methods. *Complexity, 2020*, 1-11. https://doi.org/10.1155/2020/8885861

Ajah, B. O., Ajah, I. A., & Obasi, C. O. (2020). Application of virtual reality (VR) and augmented reality (AR) in the investigation and trial of Herdsmen terrorism in Nigeria. *International Journal of Criminal Justice Sciences, 15*(1), 1-20. http://dx.doi.org/10.5281/zenodo.3792776

Aldwairi, M., & Alwahedi, A. (2018). Detecting fake news in social media networks. *Procedia Computer Science, 141*, 215-222. https://doi.org/10.1016/j.procs.2018.10.171

Aphiwongsophon, S., & Chongstitvatana, P. (2018). Detecting fake news with machine learning method. *2018 15th international conference on electrical engineering/electronics, computer, telecommunications and information technology (ECTI-CON)* (pp. 528-531). IEEE. https://doi.org/10.1109/ECTICon.2018.8620051

Batty, M. (1990). Intelligent cities: using information networks to gain competitive advantage. In (Vol. 17, pp. 247-256). SAGE Publications Sage UK: London, England. https://journals.sagepub.com/doi/pdf/10.1068/b170247

Besselaar, P. v. d., & Koizumi, S. (2005). *Digital Cities III. Information Technologies for Social Capital: Cross-cultural Perspectives: Third International Digital Cities Workshop, Amsterdam, The Netherlands, September 18-19, 2003, Revised Selected Papers*. Springer Berlin Heidelberg. https://books.google.com.pk/books?id=ly_yBwAAQBAJ

Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M., & Al Ridhawi, I. (2020). An incentive-aware blockchain-based solution for internet of fake media things. *Information Processing & Management, 57*(6), 102370. https://doi.org/10.1016/j.ipm.2020.102370

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research, 5*(4), 491-497. https://doi.org/10.1016/j.jare.2014.02.006

Hall, P. (2014). *Cities of Tomorrow: An Intellectual History of Urban Planning and Design Since 1880*. Wiley. https://books.google.com.pk/books?id=79EsAwAAQBAJ

Hardy, H., & Cheah, Y.-N. (2013). Question Classification Using Extreme Learning Machine on Semantic Features. *Journal of ICT Research and Applications, 7*, 36-58. http://dx.doi.org/10.5614/itbj.ict.res.appl.2013.7.1.3

Hartley, K., & Vu, M. K. (2020). Fighting fake news in the COVID-19 era: policy insights from an equilibrium model. *Policy Sciences, 53*(4), 735-758. https://doi.org/10.1007/s11077-020-09405-z

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in Progress: Theory and prevention of technology-enabled offenses*. Taylor & Francis. https://doi.org/10.4324/9781315775944

Ishida, T., & Isbister, K. (2000). *Digital Cities: Technologies, Experiences, and Future Perspectives*. Springer Berlin Heidelberg. https://books.google.com.pk/books?id=c8N89LbQsTQC

Jermsittiparsert, K. (2019). Behavior of tourism industry under the situation of environmental threats and carbon emission: Time series analysis from Thailand. *670216917, 9*(6), 366-372. https://doi.org/10.32479/ijeep.8365

Kolluri, N. L., & Murthy, D. (2021). CoVerifi: A COVID-19 news verification system. *Online Social Networks and Media, 22*, 100123. https://doi.org/10.1016/j.osnem.2021.100123

Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T. R., & Xiong, N. N. (2021). A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *Journal of Parallel and Distributed Computing, 152*, 128-143. https://doi.org/10.1016/j.jpdc.2021.02.022

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior, 126*, 106979. https://doi.org/10.1016/j.chb.2021.106979

Lipman, A. D., Sugarman, A. D., & Cushman, R. F. (1986). *Teleports and the intelligent city*. Dow Jones-Irwin Homewood, IL. http://sugarlaw.com/publications/teleport/teleports-all-dow-jones.pdf

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*, 191-216. https://scholarworks.gsu.edu/gpl_policybriefs/13/

Masser, I. (1990). Technology and regional development policy: a review of Japan's technopolis programme. *Regional studies, 24*(1), 41-53. https://doi.org/10.1080/00343409012331345774

Mitchell, W. J. Intelligent cities. https://uocpapers.uoc.edu/uocpapers/5/dt/eng/mitchell.pdf

Mohawesh, R., Xu, S., Tran, S. N., Ollington, R., Springer, M., Jararweh, Y., & Maqsood, S. (2021). Fake reviews detection: A survey. *IEEE Access, 9*, 65771-65802. https://doi.org/10.1109/ACCESS.2021.3075573

Okereafor, K. (2021). *Cybersecurity in the COVID-19 Pandemic*. CRC Press. https://doi.org/10.1201/9781003104124

Pattaya Mail. (2021). Pattaya mayor debunks 'fake news' about Sinopharm vaccine order. https://www.pattayamail.com/news/pattaya-mayor-debunks-fake-news-about-sinopharm-vaccine-order-366516

Porumbescu, G. A. (2018). Assessing the implications of online mass media for citizens' evaluations of government. *Policy Design and Practice, 1*(3), 233-240. https://doi.org/10.1080/25741292.2018.1507239

Rojas, H., Shah, D. V., & Faber, R. J. (1996). For the good of others: Censorship and the third-person effect. *International Journal of Public Opinion Research, 8*(2), 163-186. https://doi.org/10.1093/ijpor/8.2.163

Rygielska, M. (2020). Migrująca teranga. O współczesnych przemianach afrykańskiego systemu świadczeń całościowych we Włoszech. *socialspacejournal.eu, 19*(1), 71-88. http://socialspacejournal.eu/Social%20Space%20Journal%2012020(19).pdf#page=71

Salavrakos, I.-D. (2020). A Re-Assessment of Italian Defence Production and Military Performance in the World Wars. *Res Militaris, 10*(1). https://resmilitaris.net/index.php/2020/01/01/id1031542/

Schreuders, Z. C., Cockcroft, T., Butterfield, E., Elliott, J., & Soobhany, A. R. (2020). Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force. *International Journal of Cyber Criminology, 14*(1), 316–340. http://dx.doi.org/10.5281/zenodo.3757271

Sisaket Municipality. (2021). *Sisaket Smart City Project*. Sisaket, Thailand.

Suanpang, P., & Jamjuntr, P. (2021). A chatbot prototype by deep learning supporting tourism. *Psychology and Education, 58*(4), 1902-1911.

Suanpang, P., & Jamjuntr, P. (2021). A comparative study of deep learning methods for time-Series forecasting tourism business recovery from the covid 19 pandemic crisis. *Journal of Management Information and Decision Sciences*, 1-10. https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1543565

Suanpang, P., Netwong, T., & Chunhapataragul, T. (2021). Smart Tourism Destinations Influence a Tourist's Satisfaction and Intention to Revisit. *Journal of Management Information and Decision Sciences*, 1-10. https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1329562

Suanpang, P., Netwong, T., Keawyoung, P., Chunhapataragul, T., Nermsorn, C., Songma, S., . . . Sopa, J. (2022). *Innovation of Smart Tourism to Promote Tourism in Suphanburi Province*. Bangkok: Suan Dusit University, Thailand.

Talwar, S., Dhir, A., Singh, D., Virk, G. S., & Salo, J. (2020). Sharing of fake news on social media: Application of the honeycomb framework and the third-person effect hypothesis. *Journal of Retailing and Consumer Services, 57*, 102197. https://doi.org/10.1016/j.jretconser.2020.102197

Wemmerlöv, U. (1990). A taxonomy for service processes and its implications for system design. *International Journal of Service Industry Management, 1*(3), 0-0. https://doi.org/10.1108/09564239010002126

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access, 9*, 94318-94337. https://doi.org/10.1109/ACCESS.2021.3087109