Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
www.bircu-journal.com/index.php/birci
Budapest Institute

Use of Intelligence Based Agents to Deal with Cyber Crime

Muhamad Arif Budiman[1], Muhammad Erza Aminanto[2]
[1,2]*Universitas Indonesia*
muhaarifb30@gmail.com

Abstract

The rapid development of information and communication technology has encouraged the development of cybercrime. As a type of crime that is different from conventional crime, the handling of cybercrime requires a special way. This paper aims to examine intelligence-based agents for handling cyber crimes, Indonesia, with a focus on the use of chatbots. The method used is the library research method. Data sourced from various books, journals and internet sources were then analyzed by descriptive analysis method. The results show that the current development of AI has allowed its use to carry out crime data mining. One of the ways to do this is by using a chatbot, which is a type of intelligence-based agent. The use of chatbots in the police has the possibility to be developed as a cybercrime detection and evidence collection method. This is done by developing a chatbot framework, methodology and evidence collection procedures on the dark web and digital forensic practices.

Keywords
intelligence-based agents; chatbots; crime data mining; cybercrime

I. Introduction

The development of information and communication technology that exists today has given rise to various new challenges due to the adverse effects resulting from its misuse. This then causes various irresponsible parties to take advantage in ways that harm many people. Cyber crime is an unlawful act carried out using the internet based on technological sophistication, computers, and telecommunications, either to gain profit or not by harming other parties (Marufah, Rahmat, & Widana, 2020). This crime involves various forms of crime related to the confidentiality, integrity and existence of data and computer systems (Chintia, Nadiah, Ramadhani, Haedar, & Febriansyah, 2019).

The number of cyber crimes that occur in Indonesia cannot be said to be small. Based on data held by the National Cyber and Crypto Agency (BSSN) shows that there were 888 million cyber attacks that occurred in Indonesia from January to August 2021 (Mashabi, 2021). This then shows the severity of cybercrimes that have occurred in Indonesia. The Indonesian government did not remain silent and made various efforts to be able to deal with cyber crimes in Indonesia. This is done by issuing Law number 11 of 2008 concerning Information and Electronic Transactions which has been updated by Law no. 19 of 2016. The legislation was then used as the basis for handling cyber crimes in Indonesia.

In addition to these legal products, the Indonesian National Police has carried out law enforcement as the Indonesian police force to handle cyber crimes. One way to do this is by establishing the Directorate of Cyber Crime (Dittipidsiber) which is a work unit under the Criminal Investigation Unit of the Police and has the task of enforcing the law against cyber crimes. In addition, the National Police also makes efforts to optimize the quality of the cyber crime investigation process by conducting training for its members (Nahwan, Nurhayani,

Nugroho, & Sripure, 2021). However, it seems that these efforts still need to be improved and encouraged by other strategies.

Based on research conducted by Noviantini, Teenager, and Mariadi (2021), the police are not yet optimal in handling cyber crimes, coming from law enforcement factors. This is mainly related to special education which is not yet owned by the special cyber function unit. In addition, there is a need for more adequate facilities and infrastructure, especially in the regions to be able to improve the smooth process of investigating cyber crimes. The most needed facilities and infrastructure are digital forensic laboratories which are considered to have a major role in investigating various cyber crimes.

Cyber crime is a type of crime that requires special attention because it has a different character from conventional crimes (Chintia, Nadiah, Ramadhani, Haedar, & Febriansyah, 2019). Cybercrime should be the main focus of law enforcement agencies. In this regard, various government agencies in the security sector, along with intelligence services need to collaborate with technically skilled experts in order to adopt and frame new emerging technologies to tackle various types of cybercrime. Cyber security can then be achieved by planning and implementing appropriate strategies to address cybercrime problems (Almansoori, Alshamsi, Abdallah, & Salloum, 2021). Anticipation of these crimes include functioning of legal instruments effectively through law enforcement (Tumanggor, 2019). This means that in legal cases, the State is not present when the people need protection from any existing crime (Arifin, 2020). Crime is a negative externality with enormous social Costs (Campbell-Philips, 2020).

The development of artificial intelligence (AI) has now led to various conveniences by providing intellectual operating systems and digital assistants. Utilization of AI has even made it possible for robots to perform basic police functions. Currently the police are already using robots to carry out search and rescue operations, to dispose of explosives in terrorist activities and even to destroy armed criminals (Radulov, 2019). Moreover, due to the wide development of AI itself, AI has evolved so that it can be used in various forms. The AI paradigm has transformed police, surveillance, and criminal justice practices through dispersed monitoring modalities based on prediction and prevention. In addition, this can then be used to deal with cyber crimes. Research conducted by Sivčević, et.al (2020) shows that it is possible to use intelligence-based agents to perform electronic public services using appropriate artificial intelligence such as chatbots. Based on this research, it is also possible for the police to use intelligence-based agents to handle cyber crimes.

This paper aims to analyze the use of intelligence-based agents for handling cyber crimes in Indonesia with a focus on the use of chatbots. This paper contributes to the literature by providing insight into the possible use of chatbot-based intelligence agents in cybercrime detection through data mining. This paper will be arranged in order in the next section explaining the method used. After that, the findings and discussions will be explained, and the last section will explain the conclusions of the study.

II. Research Methods

The research method used to compose this paper is library research. This is done by collecting various reading references that are relevant to the problem under study, then understanding it carefully and carefully so as to obtain research findings (Zed, 2003). Data were collected from various literatures such as books, journals both nationally and internationally, as well as internet sources. This is then followed by an analysis carried out using a descriptive analysis method. Based on the analysis method, the observational data is poured into the form of a thesis to describe the problems studied.

III. Discussion

3.1 Artificial Intelligence and Crime Prevention

Artificial intelligence refers to the simulation of human intelligence on machines programmed to think humans and imitate their actions, the characteristic of AI itself is its ability to rationalize and take actions that have the best chance of achieving certain goals (Rachmadie, 2020). This is then utilized in the security sector to collect, sort, and manage data in the information space. This is then expected to be able to optimize the performance of the police in a quality, timely, and effective manner in ensuring national and civil security (Radulov, 2019).

According to Radulov (2019), there are several ways that can be used to utilize AI in crime prevention. This includes data collection, crime detection, cyber crime prevention and so on. AI is seen as helping organizations to prevent cybercrime by training them to recognize keywords or topics related to malicious content which is then used to stop potential cyber attacks. In addition, Machine Learning, computer algorithms that allow AI to perform learning has enabled AI to work with large amounts of data. This can then be used to investigate and prevent crime (Radulov, 2019).

Crime investigations and the collection of information related to criminal acts committed by the police can be carried out with the help of AI. Gathering information regarding crime situations including finding hidden links between organizations and individuals who commit crimes can be done with artificial intelligence (Radulov, 2019). This is partly thanks to the data mining function provided by AI. Data mining is defined as the identification of interesting structures in the data, in which the structures show patterns, statistical models or predictions of the data, and the relationships between parts of the data (Fayyad & Uthurusamy, 2002).

Data mining can then be used for crime detection, prevention, and eradication. Research conducted by Chen, et al. (2003) mentions that crime data mining can be used for entity extraction for police narrative reports, detecting criminal identity fraud with an algorithmic approach, authorship analysis in cyber crime, and analysis of criminal networks. With regard to cybercrime, activities in cyberspace are mostly anonymous, which makes the handling of cybercrimes more complicated and must rely on manual efforts. However, this is very limited by the number of messages and the perpetrator ID is constantly changing. Therefore, it is proposed for an authorship analysis framework that can be used to automatically trace the identity of cyber criminals through the messages they post on the Internet. Based on the framework, three types of message features, including stylistic markers, structural features, and content-specific features, were extracted and an inductive learning algorithm was used to build a feature-based model to identify illegal message autoships (Chen, et al., 2003).

3.2 Intelligence Based Agents

In general, the term “agent” can be seen as an entity that performs certain activities on behalf of a person. Agents generally refer to entities that operate independently in an environment, adapt to that environment, have the ability to understand the environment, change the state of that environment, and have the ability to learn (Kuk, Stanojević, Jovanović, & Nedeljković, 2018). Agents can be distinguished according to several criteria. Agent operations can be reviewed in a given environment. The state of the environment changes as it interacts with the environment. The characteristics of intelligence-based agents according to Sivčević, et.al (2020) can be seen in Table 1.

Table 1. Characteristics of Intelligence-Based Agents

Characteristics	Definition	Type
Mobile	Agents can move from one network node to another. data, namely internal attributes that represent the knowledge possessed by agents	Mobile agent
Rationality	The agent must always take the action that will maximize the expected results, thereby using his or her own knowledge of the current and future state of the environment	Rationality agent
Benevolence	Agent targets must not conflict with each other if agents are expected to maximize the expected outcomes.	Hybrid agent

Source: (Sivčević, Košanin, Nedeljković, Nikolić, Kuk, & Nogo, 2020)

The use of artificial intelligence-based agents include the following (Piscopo, Siebes, & Hardman, 2017):

1. Chatbots: AI can be used to understand everyday communication patterns using chatbots;
2. Adaptive Traffic Signals: City traffic can definitely affect our lives, traffic flow and sensors can improve the functioning of public transport;
3. Surveillance and Security: The presence of cameras has made public safety improvements, reduced the crime rate of Smart police services, and caught terrorists. Machine learning and AI will help improve facial recognition, tracking and other aspects of security detection;
4. Water and Electricity: AI is being applied to water metering to curb excess water and find leaks. Cities use smart grids/grid to better manage power;
5. Public Security: can be completely revolutionized if law enforcement agencies apply predictive modeling and AI frameworks to run checks against criminal databases. License plate reader (LPR) technology can be used by police to locate stolen cars and identify expired registrations.

3.3 Utilization of Chatbot-Based Intelligence Agents in Cyber Crime Detection

Automated conversational agents or chatbots are computer systems that imitate natural conversations with human users through images and written or spoken language (Laranjo, et al., 2018). The emergence of these chatbots represents the latest advances in AI that are enabling more natural interactions between humans and their machine-agent counterparts. This human-machine communication is becoming more complex and sophisticated, mainly through the advancement of machine learning with the application of neural networks. This is reflected in the growing number of chat agents aiming for human-like exchanges in areas such as e-commerce, travel, tourism and healthcare. Well-known examples of such intelligent chatbots are Microsoft Cortana, Amazon Alexa, or Apple Siri (Schachner, Keller, & Von Wangenheim, 2020).

Based on research conducted by Sivčević, et.al (2020) the application of chatbots in the police can have an effect on increasing the level of trust of citizens in the police. The implementation of chatbots in police work will completely change the communication between citizens and police authorities. This is because chatbots have revolutionized human interaction, namely between civilians and police. Therefore, with a chatbot, civilians and police can communicate in natural language. A chatbot can be a rule-supported and sometimes artificial intelligence service that interacts with the public via a chat interface. Chatbots can improve police-community relations and gain efficiency in the process of receiving calls with callers.

But then the use of chatbots in the police has the possibility to be developed as a cyber crime detection. It is based on the idea that automated chatbots can act independently and

learn from their own experiences and can create new crime prevention strategies. Chatbots are used as secret agents to detect crimes. In this way, chatbots which are usually used for customer service purposes, request routing, information gathering can then be expanded into criminal investigations and identification of potential criminals (Stănilă, 2020).

Based on this, Gendi and Muntenau (2021) propose to apply the interaction between the three domains to describe the feasibility of using chatbots for crime detection and evidence gathering. This interaction can be seen in Figure 1. In this case, it is proposed to implement a chatbot in three main ways, namely the use of chatbots on the dark web, methodologies and procedures for collecting evidence on the dark web, and the use of chatbots for evidence collection and digital forensic practice. The implementation of chatbots on the dark web can enable quick access to data, evaluation of information, and execution of tasks. By implementing a chatbot on the dark web, one can immediately detect volatile URLs and quickly disappear (Gendi & Munteanu, 2021). This means that cybercrime searches can be done in an easier way by utilizing chatbots.

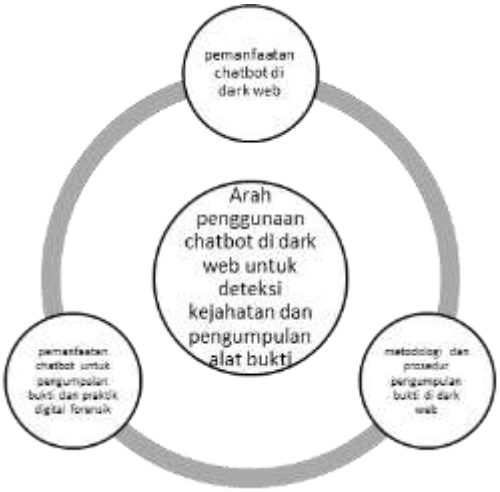

Figure 1. *The Interaction of Three Domains to Illustrate the Feasibility of Using Chatbots on the Dark Web for Crime Detection and Evidence Gathering (Gendi & Munteanu, 2021)*

Moreover, by implementing chatbots on the dark web, one can facilitate efficient sharing of information while minimizing the technical skills required for data and information collection. Lastly, as a practical implementation of AI, chatbots can be used to detect criminal activity. In particular, Gendi and Muntenau (2021) argue that chatbots can be implemented with the aim of gathering records of illegal activities and identifying perpetrators in their operations. The exploitation of the chatbot function can also be carried out with intelligent data analysis in various fields of police activity. Police analysis of data collected by artificial intelligence-based agents can be exploited to carry out data collection and analysis of criminal activities (Sivčević, Košanin, Nedeljković, Nikolić, Kuk, & Nogo, 2020).

IV. Conclusion

Cybercrime is a type of crime that is different from conventional crime. Therefore, it requires different handling efforts. This paper has reviewed the use of intelligence-based agents for handling cyber crimes, especially by using chatbots. The review shows that the current development of AI has made it possible to use it to carry out crime data mining. Intelligence-based agents can be used for this, especially chatbots that can function to understand everyday communication patterns. Chatbot within the police has the possibility to

be developed as a cyber crime detection. This can be done by developing a framework to be able to take advantage of chatbots on the dark web, apply it as a methodology and evidence collection procedure on the dark web, and use chatbots for evidence collection and digital forensic practice. In this way, the chatbot can then function as a cyber crime detection and means of collecting evidence.

References

Almansoori, A., Alshamsi, M., Abdallah, S., & Salloum, S. A. (2021). Analysis of Cybercrime on Social Media Platforms and Its Challenges. The International Conference on Artificial Intelligence and Computer Vision (pp. 615-625). Springer, Cham.

Arifin, M. (2020). The Efforts of Islamic Criminal Law Integration into Indonesian Law Procedures. Budapest International Research and Critics Institute-Journal (BIRCI-Journal) Vol 3 (2): 975-984.

Champbell-Phillips, S. (2020). Exploring Social Problems in Tobago. Budapest International Research and Critics Institute-Journal (BIRCI-Journal) Vol 3 (3): 1594-1598.

Chen, H., Chung, W., Qin, Y., Chau, M., Xu, J. J., Wang, G., et al. (2003). Crime data mining: an overview and case studies. In. Proceedings of the 2003 annual national conference on Digital government research (pp. 1-5). Texas: University of Arizona.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., & Febriansyah, A. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. JIEET (Journal of Information Engineering and Educational Technology) 2(2), 65-69.

Fayyad, U., & Uthurusamy, R. (2002). Evolving data mining into solutions for insights. Communications of the ACM, 45(8), 28-31.

Gendi, M., & Munteanu, C. (2021). Towards a chatbot for evidence gathering on the dark web. In CUI 2021-3rd Conference on Conversational User Interfaces, 1-3.

Kuk, K., Stanojević, A., Jovanović, M., & Nedeljković, S. (2018). Intelligent e-service for detecting malicious code based agent technology. Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics, (pp. 1-6).

Laranjo, L., Dunn, A. G., Tong, H. L., Kocaballi, A. B., Chen, J., Bashir, R., et al. (2018). Conversational agents in healthcare: a systematic review. Journal of the American Medical Informatics Association, 25(9), 1248-1258.

Marufah, N., Rahmat, H. K., & Widana, I. D. (2020). Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia. NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7(1), 191-201.

Mashabi, S. (2021, Sep 14). BSSN: Hingga Agustus 2021 Tercatat 888 Juta Serangan Siber. Retrieved Okt 27, 2021, from kompas.com: https://nasional.kompas.com/read/2021/09/14/10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber

Nahwan, D., Nurhayani, N., Nugroho, I. S., & Srimurni, R. R. (2021). Analisa Manajemen Strategis Program Pelatihan SDM TIK Polri dalam Menghadapi Kejahatan Siber Era 4.0. Media Nusantara, 18(2), 133-144.

Noviantini, N., Remaja, I. N., & Mariadi, N. N. (2021). Efektivitas Patroli Siber Dalam Mengungkap Kasus Ujaran Kebencian Di Wilayah Hukum Polres Buleleng. Kertha Widya, 9(1), 28-51.

Piscopo, A., Siebes, R., & Hardman, L. (2017). Predicting sense of community and participation by applying machine learning to open government data. Policy & Internet, 9(1), 55-75.

Rachmadie, D. T. (2020). Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016. Jurnal Hukum Pidana dan penanggulangan Kejahatan, 9(2), 128-156.

Radulov, N. (2019). Artificial intelligence and security Security 4.0. Security & Future, 3(1), 3-5.

Schachner, T., Keller, R., & Von Wangenheim, F. (2020). Artificial intelligence-based conversational agents for chronic conditions: systematic literature review. Journal of medical Internet research, 22(9), e20701.

Sivčević, D., Košanin, I., Nedeljković, S., Nikolić, V., Kuk, K., & Nogo, S. (2020). Possibilities of used intelligence based agents in instant messaging on e-government services. 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-5). IEEE.

Stănilă, L. (2020). Memories of the Future-Sweetie and the Impact of the New Technologies on the Criminal Justice System. EU and comparative law issues and challenges series (ECLIC), 4, 557-575.

Zed, M. (2003). Metode Penelitian Kepustakaan. Jakarta: Yayasan Obor Indonesia.

Tumanggor, F., Muazzul, and Zulyadi, R. (2019). Handling of Narcotics Child Victims in Child Special Coaching Institutions Class I Tanjung Gusta, Medan. Budapest International Research and Critics Institute-Journal (BIRCI-Journal) Vol 2 (4): 50-55.