Journal of Integrated and Advanced Engineering (JIAE)
Vol. 2, No. 1, March 2022: 11-18
http://asasijournal.id/index.php/jiae
http://doi.org/10.51662/jiae.v2i1.34

Development of Streaming Media Security using Geolocation

Agus Sulaiman*, Marza Ihsan Marzuki
Department of Electrical Engineering, Faculty of Engineering, Universitas Mercu Buana, Indonesia

Abstract
Video streaming is digital data that is shared over the internet network. Streaming video through security protection techniques creates a security that is expected to protect intellectual property rights because there is data transfer through the internet. The use of password-based and token-based authentication is a security technology widely used in exchanging data and information between the client and server. However, this method is currently not sufficient to represent a security system using a Geographic Information System. Geolocation is a system or designation of geographic location in a world on an object that is connected via the internet network. IP geolocation can be used to define a particular IP address based on the geographic location from which the device is connected to the internet. The benefit of applying this technology is that each individual or organization can identify the location of a device connected to the internet. The study will use applied research and quantitative data with the implementation of a Geographic Information System that includes the creation of a security architecture on video streaming using Geolocation and test variables that can be used as a basis for analysis to describe the results of the testers. The test results with a random access server system from 50 countries with a blacklist and whitelist grouping mapping system show a success rate of 80%. Based on the results obtained from the use of live streaming security with Geolocation, it can be implemented to improve the security system.

Keywords:
Geographic Information System;
Geolocation;
Security;
Video Streaming;

Article History:
Received: January 13, 2022
Revised: March 6, 2022
Accepted: March 9, 2022
Published: March 18, 2022

Corresponding Author:
Agus Sulaiman,
Department of Electrical Engineering, Faculty of Engineering, Universitas Mercu Buana, Indonesia
Email:
agussulaiman08@gmail.com

INTRODUCTION

In recent years, streaming electronic media has become a social phenomenon of global economic [1]. Streaming electronic media has the meaning of data which is usually seen in the form of streaming audio and video over the internet network in the form of compressed data and is received by the user for display [2][3]. Video streaming has Quality of Service (QoS) standards. QoS is an important criterion for network applications that require real-time streaming [4][5]. QoS video streaming is the benchmark in providing better visual quality with a low file size which saves storage and easily streams on slow networks without buffering/delays [6]. However, apart from QoS, some things need to be considered in the video streaming process information data security [7, 8, 9].

In an era that has seen tremendous progress in information and communication technology (ICT), data security seems to be more vulnerable than ever [8, 10, 11]. This is caused by technological innovation accessibility in obtaining information that goes hand in hand with security threats that come from the cyber scope [8][9]. In the modern world, where multiple applications and devices generate large amounts of data resulting in the big data phenomenon, security and protection an of paramount play importance at international, regional, and national levels. Several methods have been started and have been implemented in video security, including using password-based authentication and token-based

authentication [10, 12, 13].

Password-based authentication and token-based authentication are security technologies that exchange information data between the client and server [8]. However, this method is currently not sufficient to represent a security system using a Geographic Information System. So that in this study, we will discuss the security of illegal streaming/restream without permission by using geolocation mapping technology, where the technology can provide security by limiting visitor access rights based on the IP address that is sent to the destination streaming server [14][15].

The urgency of this research is to know the mastery and understanding of concepts in learning and aspects of streaming media technology development. In addition, the technology uses the development of a security support system using a Geographic Information System approach. The security system uses a country grouping system based on *allow* and *denny* server visitors. This is an urgency in itself, and solutions need to be found to overcome challenges as well as to resolve these problems.

The processing of the streaming media data security system is carried out based on data [16, 17, 18] input to the server in the form of IP addresses at the network layer that has been determined based on predetermined criteria [8, 17, 18]. The security of the streaming media system is expected to be used as a way to develop a security system and support and complement the existing security.

METHOD

The selection of research methods is an essential part of supporting the process's implementation steps to solve problems in research. Mastering research methods has benefits in developing the field of science that is occupied and can reproduce the results of discoveries that are beneficial to the broader community and the world of education

IP address-based geolocation is a way to be able to find the location of devices connected to the internet. In this attribute, IP addresses are used, and tools to search for geolocations are made by querying the database to obtain specific IP address information. Most geolocation databases provide the most basic information, including continents, countries, cities, approximate longitudes, and latitudes [19][20].

The utilization of these two elements will obtain information in the form of target locations. The IP address is a unique identifier for each electronic device connected to the internet network. Through IP addresses, electronic devices can connect and share data with each other. The Geolocation IP address block diagram is shown in Figure 1.

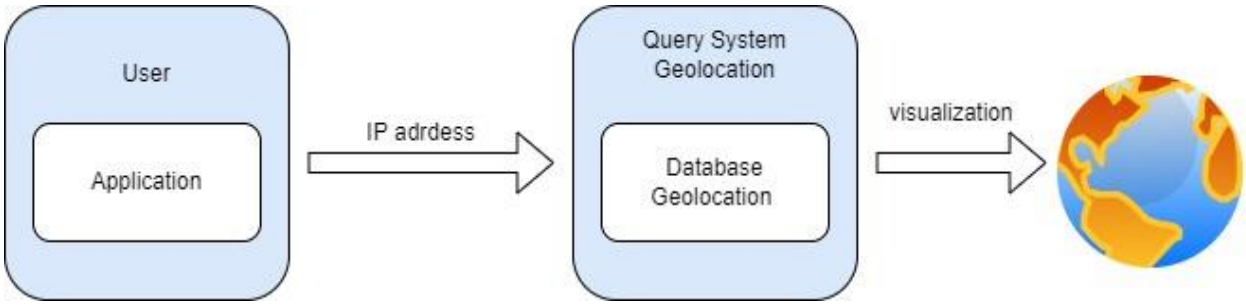

Figure 1. Geolocation IP address

Material

The Geographic Information System technology is the basis for applying the level of security in this research. Utilization of the Geographic Information System that is applied is to store information on the IP address database from several countries into one system. This storage is needed to check and map the IP address of the visitor's address based on the predefined privileges in the system [17].

The choice of geographic location in this implementation is that the accuracy of the data provided is high enough so that it can be used as a goal for data security based on geography. The source of information received by the server is in the form of the user's IP address which will be a reference in geolocation mapping. The IP address data source will provide information in the form of IP address type, continent code, continent name, country code, country name, area code, region name, city, zip, latitude, longitude [19][20].

Method

The research method that will be used in this research is to use applied research methods and quantitative data analysis techniques. Applied research is any research that aims to increase scientific knowledge with a practical purpose. The reason for using applied research is because it underlies the policy of decision-making or administrators. In terms of objectives, using applied research methods is expected to be used to benefit discoveries that like to apply certain theoretical concepts. The use of quantitative methods in this study intends to analyze the test results based on or referring to the objective data from the results of the tests carried out. Figure 2 shows the design streams using geoip database.

In this study, we will use mathematical modelling of subset notation, using the following provisions:

a. List method

List all IP addresses on the whitelist database:

A = { whitelist IP addresses }

B = { IP address blacklist }

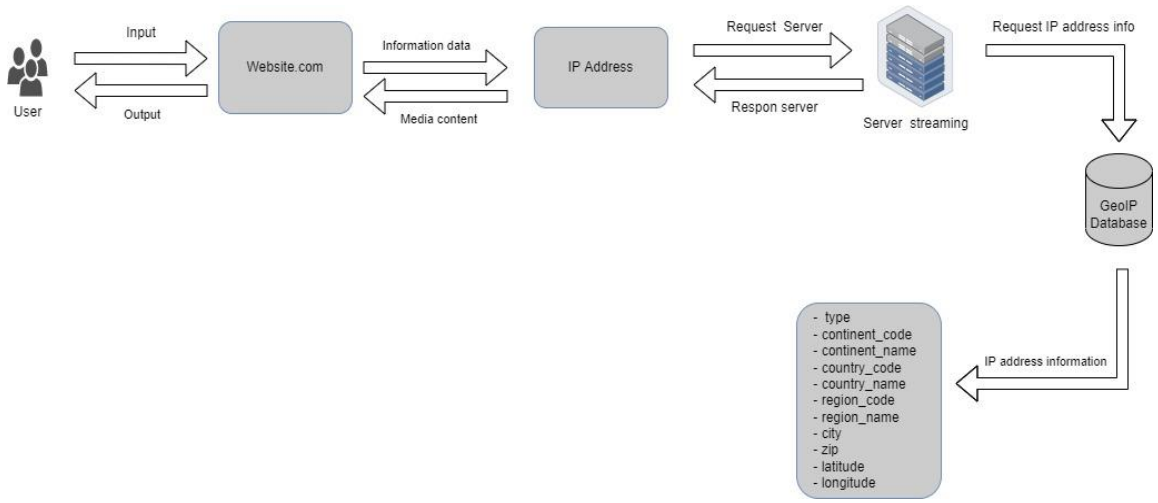

Figure 2. Design streams using geoip database

b. Method description
Using set-builder notation:
Notation: { x | conditions that must be met by x }

A = { x | x is a list of whitelisted ip addresses }
Or
A = { x | x } ip address, < whitelist }

B = { x | x is a list of ip addresses that are listed on the blacklist }
Or
B = { x | x } ip address, < blacklist }

The result of understanding the mathematical theory that has been explained under the conditions in obtaining privileges is that if the user's IP address is whitelisted, but if not, it will get a response not allowed

RESULTS AND DISCUSSION

System implementation and configuration

The implementation of the system in this study uses several tools based on open source, which can be used freely and openly to be used as system development. In the initial implementation process, several tools will be prepared in terms of system design and implementation, including using nginx streaming, IP address geolocation database, elasticsearch, kibana, logstash, and filebeat

Configuration of a system is a structured process consisting of several entities with their respective functions that interact or are interconnected to produce goals in system design and implementation. The combination and use of elasticsearch, kibana, logstash, and filebeat software in this study will be used as tools to collect data from the test results. The combination of using these tools is very useful in sending, collecting, searching, analyzing, and visualizing data. Table 1 lists the system information used in this research.

System Testing

The test scenario is needed to simulate the expected system design implementation results by the system settings that already have requirements. Therefore, the test simulation method that will be carried out is to do a simulation where several countries have entered the whitelisted category and are also listed in the blacklist category.

The test scenario will represent the decision rule as true or false, which is a technique that is generally applied when a requirement/rule is enforced. Tests that make a combination of conditions, actions, rules, and results as test requirements are performed to produce a response to the objectives of this study. This helps in identifying and validating the correct test cases.

Table 1. System Information

No.	Hostname server	Operating system	Application
1	Streaming	Ubuntu 20.04	Nginx RTMP Database geoip Filebeat
2	Datalog visualization	Ubuntu 20.04	Elasticsearch Logstash Kibana

Based on the flow of the test scenario, the simulation will be carried out by accessing servers from several regions/countries, in this case, to create a mapping of data grouping from 50 countries into two division groups. In each region, there are conditions so that the next command that will be generated is in accordance with the conditions that have been set on the streaming server system in the hope of having the same response according to the settings instructed. Based on the conditions that have been determined, it will generate two response codes, namely 200 successful and 403 prohibited. Where response 200 is the response from the whitelist while 403 is the response from the blacklist. The information regarding country data and country codes that will be used as the basis for the simulation material of this research can be presented in Table 2.

The testing process is carried out using the black box testing method. Black box testing is a functional testing method that focuses on input and output without knowing the internal structure and details of application implementation based on predetermined requirements and specifications

The results of the tests that will be used as a reference in making the final report are the collection, utilization, and filtering of log data from the streaming server, which is used as a source of visualized information data to make it easier to read the report results.

Data collection in this report uses data from mapping results from 50 countries that have been grouped based on whitelists and blacklists. Therefore, the data stored in the visualization log system is 40 countries consisting of 20 countries with whitelist groupings and 20 countries with blacklist groups.

The data will produce detailed settings for the response that has been previously determined, namely in the form of country name data, country code, response code, and unique IP address that visits the streaming server.

Table 2. Mapping IP address

Mapping IP addresses by region							
Whitelist				**Blacklist**			
Country	**Code**	**Conditions**	**Response code status**	**Country**	**Code**	**Conditions**	**Response code status**
Armenia	AM	TRUE	200 success	Austria	AT	FALSE	403 forbidden
Australia	AU	TRUE	200 success	Brazil	BR	FALSE	403 forbidden
Bangladesh	BD	TRUE	200 success	Bulgaria	BG	FALSE	403 forbidden
China	CN	TRUE	200 success	Canada	CA	FALSE	403 forbidden
Christmas Island	CX	TRUE	200 success	Denmark	DK	FALSE	403 forbidden
Hong Kong	HK	TRUE	200 success	Finland	FI	FALSE	403 forbidden
Indonesia	ID	TRUE	200 success	France	FR	FALSE	403 forbidden
Israel	IL	TRUE	200 success	France, Metropolitan	FX	FALSE	403 forbidden
India	IN	TRUE	200 success	Germany	DE	FALSE	403 forbidden
British Indian Ocean	IO	TRUE	200 success	Greece	GR	FALSE	403 forbidden
Iran	IR	TRUE	200 success	Hungary	HU	FALSE	403 forbidden
Japan	JP	TRUE	200 success	Iceland	IS	FALSE	403 forbidden
Korea, Republic of	KR	TRUE	200 success	Liechtenstein	LI	FALSE	403 forbidden
Myanmar	MM	TRUE	200 success	Luxembourg	LU	FALSE	403 forbidden
Mongolia	MN	TRUE	200 success	Latvia	LV	FALSE	403 forbidden
Malaysia	MY	TRUE	200 success	Macedonia	MK	FALSE	403 forbidden
New Zealand	NZ	TRUE	200 success	Moldova	MD	FALSE	403 forbidden
Palestinian Territory	PS	TRUE	200 success	Netherlands	NL	FALSE	403 forbidden
Russian Federation	RU	TRUE	200 success	Poland	PL	FALSE	403 forbidden
Singapore	SG	TRUE	200 success	Romania	RO	FALSE	403 forbidden
Turkey	TR	TRUE	200 success	Seychelles	SC	FALSE	403 forbidden
Taiwan	TW	TRUE	200 success	Sweden	SE	FALSE	403 forbidden
Macao	MO	TRUE	200 success	Ukraine	UA	FALSE	403 forbidden
Vietnam	VN	TRUE	200 success	United Kingdom	GB	FALSE	403 forbidden
Yemen	YE	TRUE	200 success	United States	US	FALSE	403 forbidden

For example, for groups of countries with whitelist data, a response code of 200 will be generated, which means that the IP address of the visitor's country is given access rights, while countries with a blacklisted group will produce a response code of 403, which means that the IP address of the country is not given access to obtain information from streaming data sources.

The percentage of visitors' IP addresses from several countries will also be visualized using unique IP address filtering to complete the report from the test results in tabular form. This is done to determine the total percentage of IP addresses from several countries that have visited the streaming server. The whitelist result is listed in Table 3, and the percentage is shown in Figure 3. However, Table 4 lists the blacklist result, and the percentage is depicted in Figure 4.

Table 3. Whitelist results

Top values of geoip.country_name.keyword	Top values of geoip.country_code3.keywod	Response	Unique count of clientip. Keyword
China	CN	200	20
Russia	RU	200	13
Hong Kong	HK	200	8
India	IN	200	4
Singapore	SG	200	4
Iran	IR	200	3
Macao	MO	200	3
Bangladesh	BD	200	1
Indonesia	ID	200	2
Japan	JP	200	2
Palestine	PS	200	2
Turkey	TR	200	2
Australia	AU	200	1
Malaysia	MY	200	1
Mongolia	MN	200	1
Myanmar	MM	200	1
New Zealand	NZ	200	1
South Korea	KR	200	1
Taiwan	TW	200	1
Vietnam	VN	200	1

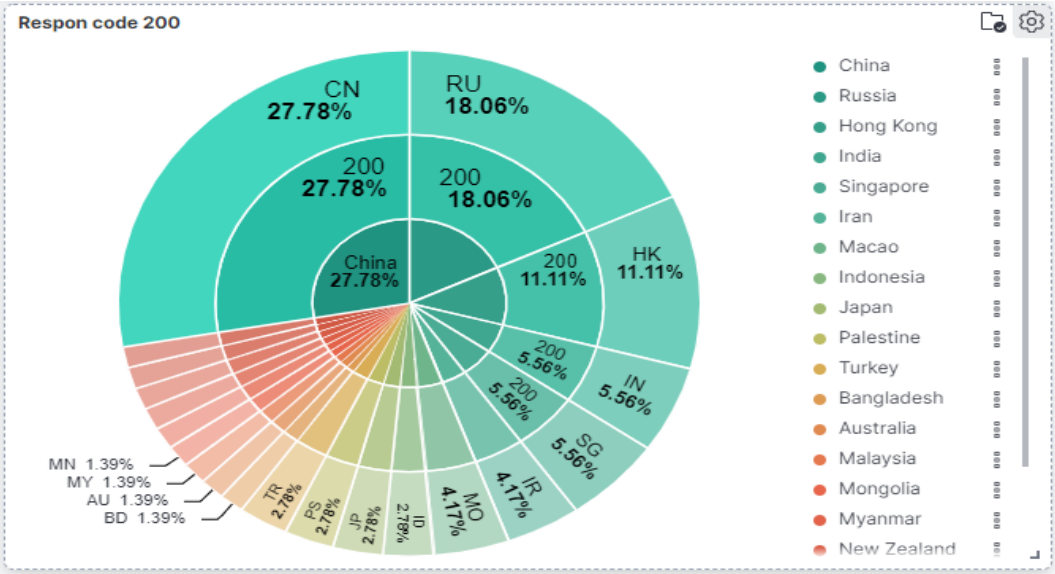

Figure 3. Whitelist results

Table 4. Blacklist results

Top values of geoip.country_name.keyword	Top values of geoip.country_code3.keywod	Response	Unique count of clientip. Keyword
United States	US	403	257
Germany	DE	403	130
Luxembourg	LU	403	98
Netherlands	NL	403	86
France	FR	403	44
Austria	AT	403	20
Switzerland	CH	403	19
United Kingdom	GB	403	16
Canada	CA	403	15
Romania	RO	403	16
Sweden	SE	403	16
Denmark	DK	403	12
Moldova	MD	403	12
Seychelles	SC	403	12
Ukraine	UA	403	12
Brazil	BR	403	7
Iceland	IS	403	7
Latvia	LV	403	6
Bulgaria	BG	403	5
Finland	FI	403	5

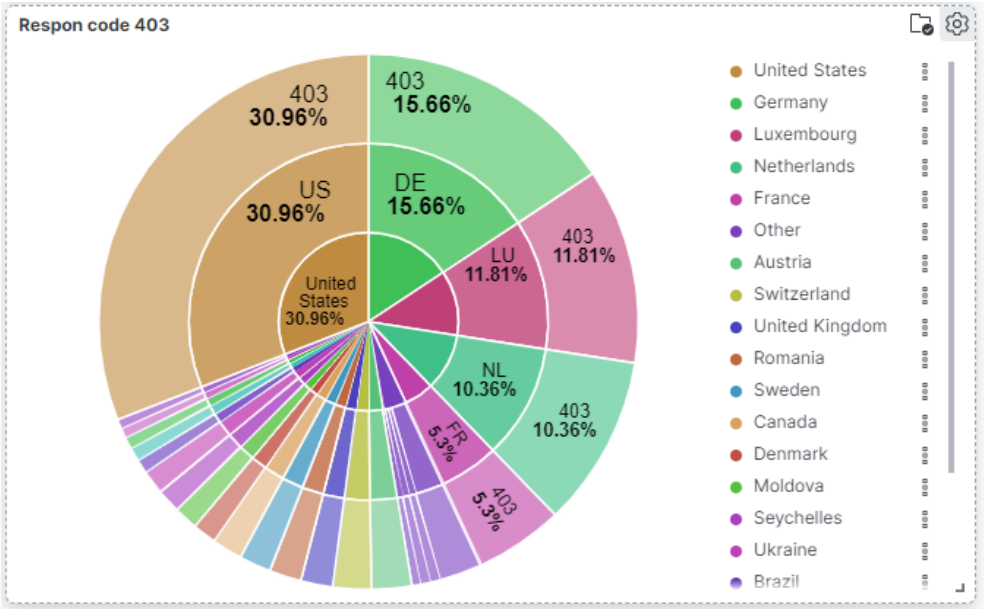

Figure 4. Blacklist results

Based on the data from the results of the two tests that have been carried out, it can be seen that the tests were carried out to meet the requirements that the system has determined. Where several countries that have been previously mapped final produce results to make video streaming security using Geolocation.

CONCLUSION

Several tests have been carried out with good results. The test focuses on simulating several variables on the mapping from 50 countries. The mapping uses random access servers in these countries. The mapping results are classified in a blocklist and a whitelist of each country. The success rate of this classifier reaches 80%. Therefore, it can conclude that Geolocation's live streaming security can be applied to help improve system security by utilizing information sources from visitors' IP addresses.

REFERENCES

[1] A. Zoellner," Trends and Perspectives on Digital Platforms and Digital Television in Europe| Commissioning and Independent Television Production: Power, Risk, and Creativity," *International Journal of Communication*, vol. 16, pp. 19, 2022.
[2] S. Zhang, G. Liu, J. Xu, and S. Wan, "Design and analysis of a fair, efficient and stable multi-server adaptive streaming protocol," *Computers and Electrical Engineering*, vol. 95, ID: 107371, 2021, doi: 10.1016/j.compeleceng.2021.107371
[3] A. Firdausi et al., "Design of A Dual-Band Microstrip Antenna for 5G Communication," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 1, no. 1, pp. 53-64, 2021, doi: 10.51662/jiae.v1i1.13
[4] M. Zhang et al., "Smart collaborative video caching for energy efficiency in cognitive Content Centric Networks," *Journal of Network and Computer Applications*, vol. 158, ID: 102587, 2020, doi: 10.1016/j.jnca.2020.102587Get
[5] J. Räsänen, A. Altonen, A. Mercat and J. Vanne, "Open-source RTP Library for End-to-End Encrypted Real-Time Video Streaming Applications," *2021 IEEE International Symposium on Multimedia (ISM)*, 2021, pp. 92-96, doi: 10.1109/ISM52913.2021.00023.
[6] S. Karim, H. He, A. A. Laghari, and H. Madiha, "Quality of Service (QoS): Measurements of Video Streaming*," IJCSI International Journal of Computer Science Issues*, vol. 16, no. 6, pp. 1694-0784, 2019, doi: 10.5281/zenodo.3987056
[7] A, P. Kirilenko, "Geographic Information System (GIS): Making Sense of Geospatial Data," *Applied Data Science in Tourism*, pp. 513-526, Springer, Cham, Germany, 2022, doi: 10.1007/978-3-030-88389-8-24
[8] H. Li, C. Yang and J. Liu, "A novel security media cloud framework, *Computers & Electrical Engineering*, vol. 74, pp. 605-615, 2019, doi: 10.1016/j.compeleceng.2018.07.022
[9] A. L. S. Orozco et al., "A machine learning forensics technique to detect post-processing in digital videos," *Future Generation Computer Systems*, vol. 111, pp. 199-212, 2020, doi: 10.1016/j.future.2020.04.041
[10] I. Capuni, N. Zhuri and R. Dardha, "*TimeStream: Exploiting video streams for clock synchronization," Ad Hoc Networks*, vol. 91, 2019, doi: 10.1016/j.adhoc.2019.101878
[11] S. Sultan and C. D. Jensen, "Metadata based need-to-know view in large-scale video surveillance systems," *Computer and security*, vol. 111, no. 4, ID: 102452, 2021, doi: 10.1016/j.cose.2021.102452
[12] L. Du et al., "An efficient privacy protection scheme for data security in video surveillance*," Journal of Visual Communication and Image Representation*, vol. 59, pp. 347-362, 2019, doi: 10.1016/j.jvcir.2019.01.027
[13] R. Muwardi et al., "Network Security Monitoring System Via Notification Alert," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 1, no. 2, pp. 113-122, 2021, doi: 10.51662/jiae.v1i2.22
[14] A. F. Lukasheh, R. L. Droste, and M. A. Warith, "Review of Expert System (ES), Geographic Information System (GIS), Decision Support System (DSS), and their applications in landfill design and management," *Waste Management & Research: The Journal for a Sustainable Circular Economy*, vol. 19, no. 2, pp. 177-185, 2001, doi: 10.1177/0734242X0101900209
[15] S. Abdollahi, M. Madadi and K. Ostad-Ali-Askari, "Monitoring and investigating dust phenomenon on using remote sensing science, geographical information system and statistical methods," Applied Water Science, vol. 11, 2021, doi: 10.1007/s13201-021-01419-z
[16] Y. Wang, X. Zhao and Y. Cao, "Detecting the fingerprint of video data hiding tool OpenPuff," *Forensic Science International Reports*, vol. 2, ID: 100088, 2020, doi: 10.1016/j.fsir.2020.100088
[17] P. Zola, C. Ragno and P. Cortez, "Google Trends spatial clustering approach for a worldwide Twitter user geolocation," *Information Processing and Management*, vol. 57, no. 6, ID: 102312, 2020, doi: 10.1016/j.ipm.2020.102312
[18] A. Dvir et al., "Encrypted video traffic clustering demystified," Computers and Security, vol. 96, ID: 101817, 2020, doi: 10.1016/j.cose.2020.101917
[19] X. Luo et al., "An overview of microblog user geolocation methods," *Information Processing and Management*, vol. 57, no. 6, ID: 102375, 2020, doi: 10.1016/j.ipm.2020.102375
[20] X. Liu et al., "A State-of-the-Art Review on the Integration of Building Information Modeling (BIM) and Geographic Information System (GIS)," *ISPRS International Journal of Geo-Information*, vol, 2, no. 2, pp. 53, 2017, doi: 10.3390/ijgi6020053