Hindawi
Complexity
Volume 2020, Article ID 6690569, 12 pages
https://doi.org/10.1155/2020/6690569

Research Article

Identification of Attack on Data Packets Using Rough Set Approach to Secure End to End Communication

Banghua Wu,[1] **Shah Nazir**,[2] **and Neelam Mukhtar**[3]

[1]*College of Cybersecurity, Sichuan University, Chengdu 610041, China*
[2]*Department of Computer Science, University of Swabi, Swabi, Pakistan*
[3]*College of Home Economics, University of Peshawar, Peshawar, Pakistan*

Correspondence should be addressed to Banghua Wu; wubh@motherchildren.com

Received 10 October 2020; Revised 26 October 2020; Accepted 2 November 2020; Published 12 November 2020

Academic Editor: M. Irfan Uddin

Security has become one of the important factors for any network communication and transmission of data packets. An organization with an optimal security system can lead to a successful business and can earn huge profit on the business they are doing. Different network devices are linked to route, compute, monitor, and communicate various real-time developments. The hackers are trying to attack the network and want to draw the organization's significant information for its own profits. During the communication, if an intrusion or eavesdropping occurs, it will lead to a severe disfigurement of the whole communication network, and the data will be controlled by wrong malicious users. Identification of attack is a way to identify the security violations and analyze the measures in a computer network. An identification system, which is effective and accurate, can add security to the existing system for secure and smooth communication among end to end nodes and can work efficiently in the identification of attack on data packets. The role of information security is to design and protect the entire data of networks and maintain its confidentiality, integrity, and availability for their right users. Therefore, there is a need for end to end security management, which will ensure the security and privacy of the network and will save the data inside networks from malicious users. As the network devices are growing, so the level of threats is also increasing for these devices. The proposed research is an endeavor toward the detection of data packets attack by using the rough set theory for a secure end to end communication. The experimental work was performed by the RSES tool. The accuracy of the *K*-NN was 88% for the total objects of 8459. For cross validation purposes, the decision rules and decomposition tree algorithms were used. The DR algorithm showed accuracy of 59.1%, while the DT showed accuracy of 61.5%. The experimental results of the proposed study show that the research is capable of detecting data packets attack.

1. Introduction

The information technology played a significant role in real life and has made the life stress-free. With the advancements and developments of information technology, security has been considered as one of the main fears for interaction and communication [1–10]. Within the last decade, the information security attacks become upraised, and hackers tried to apprehend the origination significant information for their personal profits. This kind of attack on information and network can severely put the proprietor of network and information into huge damage. Security of network and information of an organization is extremely reliant on diverse forms of information of the organization. Security has become one of the significant factors for any communication and transmission of data. Different smart devices are linked to process, communicate, monitor, and compute various real-time developments. Through the interaction and communication, if an eavesdropping occurs, then it will lead to a severe damage of the whole networks, and the data will be controlled by immoral spiteful users. Identification of attack is a way to identify the security violations and analyze the measures in a computer network.

In modern day industry of information communication, the devices are connected through the Internet of Things (IoT) forming a network of communication. Due to the

challenges of security and privacy, the idea of IoT came into existence. The reason was that the conventional protocol of security does not support security of the IoT devices. Researchers have proposed the use of diverse approaches and measures of security for securing the information and their communication and to further secure the network [10–18]. These measures include logical access, firewalls, identification, control, authentication, and encryption and decryption. Building a complete security system is hard to accomplish, and not any of these measures of security only can secure the network communication [11, 18]. An identification system, which is accurate and effective for malicious activities or intrusion detection, can further secure the prevailing system for secure and smooth communication of end to end nodes. The role of information security is to design and protect the entire data of networks and to maintain its confidentiality, integrity, and availability for their right users. Therefore, there is a need for end to end security management, which will confirm the security and privacy of the network and will save the data inside networks from malicious users. As the number of devices connected to a network is growing with the passage of time. So, the level of threats is also increasing for these devices.

To overcome the problem of the severity of security, the planned study has implemented the approach of rough set, which is a mathematical tool that can deal with the situation of uncertainty for the identification of attack for data packets and ensure the secure communication of end to end nodes. The dataset available at Kaggle [19] "Attack Prediction on Data Packets" was used to validate the research. The experimental results of the study show the acceptance and success of the study in the detection of attacks on packets of data.

The organization of the paper is as follows; section 2 shows the literature and related work to the current research, in particular, identification of attacks on data packet. Section 3 briefly presents the library-based analysis of the available literature from diverse viewpoints in the utmost widespread libraries and the applications of rough set to the proposed study. The experimental results and discussions are given in section 4. The paper is concluded in section 5.

2. Related Work

Researchers are trying to come across diverse techniques, approaches, tools, and solutions for the identification and prevention of security attacks. Kotenko and Chechulin [20] offered a security evaluation framework and attack modelling in event management and security information system. Subsorn and Limwiriyakul [21] observed the Internet banking security of 16 Australian banks for identifying the insufficiencies, which were possibly disturbing the bank customers' confidentiality. Besides, the research examined 12 Thai commercial banks and matched the experimental results with the prior research studies. Kotenko and Chechulin [22] planned an approach to the computer modelling attack and security evaluation to comprehend the event management and security information system. The authors planned a quantitative method for information systems security risk, which is systematic, modular, and extendable. The research aimed to efficiently estimate the threats of security in a wide-ranging manner [9]. Manjiatahsien et al. [23] elaborated a summary of the architecture of IoT with comprehensive details on machine learning algorithms and implications of the IoT security with various attack types. The research presented an approach of the related factors of information management for the organization of information security. Initially, 136 articles were surveyed for identifying the factors of information security, and then a sequence of interviews were performed with 19 experts of the industry for evaluating the association of these factors. In the third step, a comprehensive model was developed [24].

The detection and measurement of security have important role in the areas such as IoT in smart city. The authors [25] accompanied a comprehensive review of the literature of deep learning, IoT security, and technologies of big data. Zhang et al. [7] suggested a method for crowed measuring the trustworthiness and security of open social networks on the basis on signaling theory. The devices of IoT functioning in the environment of healthcare are vulnerable to numerous attacks and cyber threats. The industry of healthcare faces 340% issues of security, and it is 200% extra vulnerable to theft of data [26]. Accordingly, over 90% of enterprises have faced security breach [27]. Additionally, the research recommended that there is typical of 164 cyber threats identified per 1,000 linked host devices in the system of Internet of Medical Things [28]. The devices of IoMT are organized in a system deprived of considering the security, and this is the key motive that these devices grieve from availability, integrity, and confidentiality issues [29]. These susceptibilities permit the cyber-criminals to acquire access into the network of the IoMT and attain the sensitive and particular data regarding the patient. The key issues confronted by the devices of IoMT are privacy and security. Jhonson and Jhonson presented that the devices of the IoMT such as digital insulins are susceptible to cyber threats [30]. In the system of IoHT, the data applicable to the patient is stored in the cloud and is transformed back and forward from side to side through millions of devices of the IoT, and thus it spawns the susceptibility to data in their application. Due to the susceptibility, many enterprises may not agree to store the applications of IoT on the cloud. Thus, risk evaluation is required preceding the storage of such applications on the cloud and for devices of mobile mounting the applications of IoT [31]. Occasionally, decision-making about the choice of top security for the devices of the IoHT is an issue due to numerous factors involving such growing multifaceted measures relating to security, vast amount of heterogeneous devices of IoT, processing limitations, and capability of memory of such devices. Considering these situations, deficiency of appropriate security measures and criteria is not a worthy style.

The study [5] offered a comprehensive summary of security belongings analysis of ML algorithms. They examined the security of ML to build up an outline for diverse areas of researches. The attack approaches and conferring the approaches of defense alongside them were done. The research offered an outline of the strengths and flaws of the

existing assessment approaches for security and usability of the websites of E-commerce. The assessment models from 2000 to 2018 have been studied for E-commerce [32]. Mao et al. [33] planned a security dependency system for measuring the implications of security system from extensive viewpoints of the system. Nazir et al. [10] devised an approach to assess software components security through the analytic network process. They elaborated that the technique is effective and efficient in circumstances of complexity where the dependencies exist amongst diverse network nodes.

The appearance of deep learning has transformed the field of research to support practitioners and researchers with programmed feature extraction capabilities [34]. These programmed feature extraction abilities not only allow the practitioners and researchers to get free of the difficulty of picking important feature extraction approach pertinent to a certain issue, but also confirm the huge recognition rate related to conformist algorithms of classification. Schuster and Paliwal [35] suggested the Bidirectional Recur-rent Neural Network after scheming RNN in a forward and a backward direction. This is acceptable preserving lengthy series situation information about past and future through Bidirectional Long Short Term Memory [36]. The grouping of attributes of BRNN and LSTM models is collectively known as BLSTM.

3. Research Method

In the recent few years, attacks on information and network security grew. The intruders are endeavoring to take significant information from the organizations for their use and profits. These security attacks on networks and their data can severely place the proprietor of network and information into huge damage. The organization security of information is extremely reliant on diverse sorts of information of the organization. Security has become one of the significant factors for any communication and transmission of data. Different smart devices are linked to process, communicate, monitor, and compute various real-time developments. During communication and transmission, if any intrusion or eavesdropping occurs, then it is harmful for the owners of information network and can then lead to a thoughtful mutilation of the whole network, and the data will be controlled by wrong malicious users. Traditionally, the computing security is always trusting the approaches and mechanisms of authentication and access control. These provide access to authorized users. Pervasive and ubiquitous computing is very flexible and scalable due to which it is not suitable to adopt such services. The information security provides services through its platforms in the form of pervasive and ubiquitous computing, which is one of the advanced paradigms of information security. Pervasive computing plays an important role in the area where it delivers capability to allocate computational facilities to the atmospheres where people work and lead to make concerns like identity, privacy, and trust. The key benefits of pervasive computing are the design and development of services that are efficient to the users, who send query as request for the services and in situations from which the service request is sent. Figure 1 depicts flowchart for conducting the study.

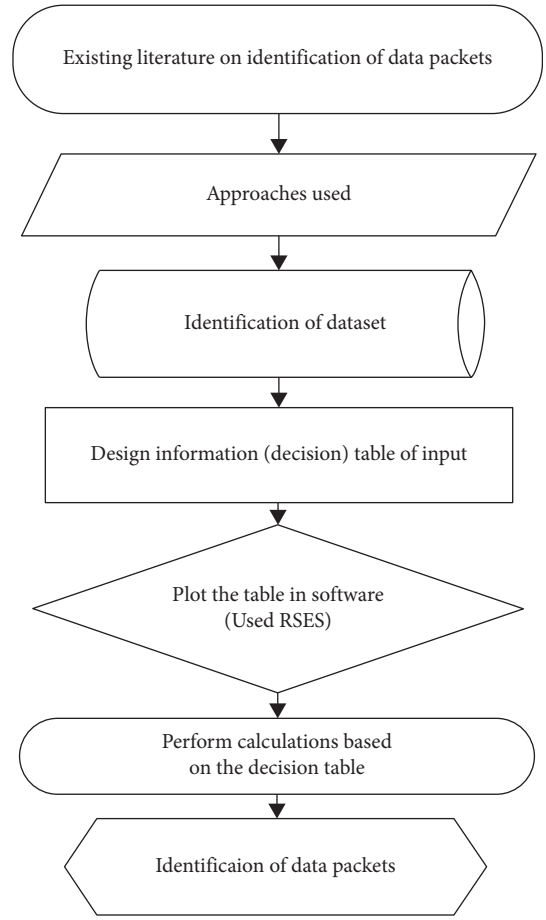

Figure 1: Flowchart of the proposed study.

The contribution of the proposed study is to adopt a rough set approach. A mathematical tool for dealing with uncertainty arises in the detection of attacks on data packets. The dataset available online at Kaggle was used to validate the research process. The approach demonstrates the accomplishment in attack identification of data packets for secure communication of end to end nodes. The figure consists of different phases. In the first phase, the existing literature is studied in order to show the related work in the area. In the next phase, the details of the approaches used in the area are given. In the third phase, the dataset was identified for conducting experiments of the proposed study. In the fourth phase, the information (decision) table was designed from the dataset. In the fifth phase, the information table was inserted into the RSES tool in order to do the experiment on the dataset. In the sixth and final phase, the process of cancelation was done through the software in order to apply algorithms and obtain results. The following subsections show the research methodology in brief.

3.1. Search Strategies of the Existing Research. The recent developments in IT sector have made the world move from huge systems and have a propensity to controlling and reduced devices for facilitating interfaces of heterogeneous and huge computational wireless communications. Security

is a key part of a system for its smooth functionality. Diverse methods and approaches are used for securing the communication inside and outside the network. Identification of attack is a way to identify the security violations and analyze the measures in a computer network.

The devices of IoT are always vulnerable due the situation in which they are operating. The associated IoT devices are mobile devices and could drop connectivity due to vulnerability of wireless outages. According to [37–39], the common IoT vulnerabilities are identified and presented in Figure 2.

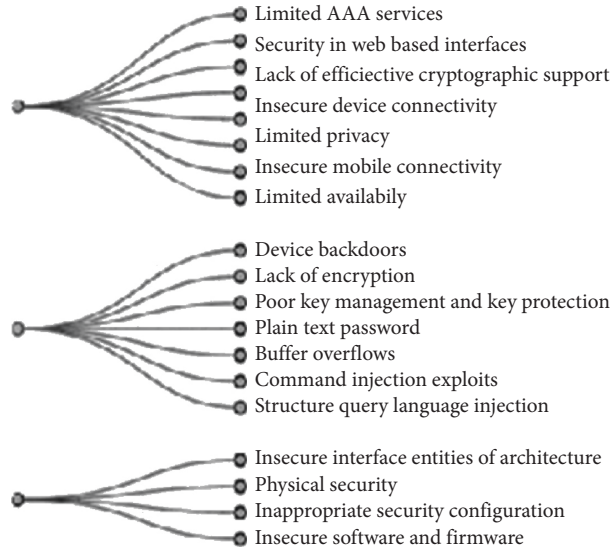

Figure 2: IoT vulnerabilities.

The strategy of search was adopted to know about the existing literature in the field. For this purpose, the popular libraries in the field such as ACM, IEEE, Sciencedirect, and Springer were searched. The data from these libraries were collected in the form of year of publication, type of publication, the areas of publication, media of publication, and other types of studies that are given in figures and tables. Figure 3 presents magazine/journal names and articles published in the library of ACM. The search process shows several materials in different forms including conference papers, journal papers, books, and many other online materials. The purpose of these materials was to show the background knowledge in the area of security for end to end communication.

Figure 4 presents the number of publications along with the media format in which the paper is published. These categories include PDF, image, HTML, video, and other formats.

Figure 5 shows all the publications along with the total number of papers published for the search process in the ACM library. These publications are in the form of journal, conference, book, and other types.

The publications categories were further elaborated to show in depth details of the associated studies. Figure 6 presents the types of contents and number of articles published. The figure depicts that more papers were published in the form of research article followed by poster, and so on.

After the search process of ACM, the search was performed in the IEEE library. The reason behind searching in different libraries was to identify more details of the area in the widespread libraries. Figure 7 presents publication type along with the number of articles in the IEEE library. In this library, more papers were obtained in the form of conference papers followed by journal papers.

Figure 8 presents the topics of publications along with the total number of articles published in the IEEE library.

The figure shows different topics and areas in the field in which more work is done in the area of security of data followed by telecommunication security, and so on. The reasons behind the identification of these topics were to know which area is mostly researched.

The search process was then performed in the Sciencedirect library for identifying further the studies published in the field. This library publishes quality papers in different areas of interest. Among the available libraries, more focus was given to this library. The reasons behind the search process in this library were to identify the related materials and the research done in the field and provide background knowledge. Figure 9 shows the total number of papers published in the given year. From the figure it is concluded that there will be an increase in the number of publications in the coming year regarding the identification of security threats. In the figure, it is shown that more papers are published in last two years, which shows that there is a significant work done in the area and still the work is going on.

Figure 10 depicts the types of articles along with the total number of articles published. These types of article include the journal, conference, book, and others. This step was performed to know about the type of papers in which more focus was given to indexed journal papers.

Figure 11 shows the title of publication, and the reason of this was to know the number of publications in the area, which particular area has how much publications available online in the given title of publication. The figure shows that more work has been done in the area of computer networks followed by computer and security, then computer communication, and so on. The identification of different areas of security, type of publications, year of publication, and the publisher was quite tricky process. This was done for ensuring that most related materials in the areas should be identified to support the current study. For these reasons, different types of search mechanisms were adopted. Most of the process was done manually by the authors for ensuing that no related materials should be missed, although some of the materials that are relevant to the current study may be missed.

Figure 11 presents the publication title along with the number of articles published.

At last, the library of Springer was searched to view associated materials published related to the proposed research. Figure 12 presents the types of contents along with the number of articles in the Springer library.

Figure 13 presents the disciplines in which the papers are published along with the number of articles published.

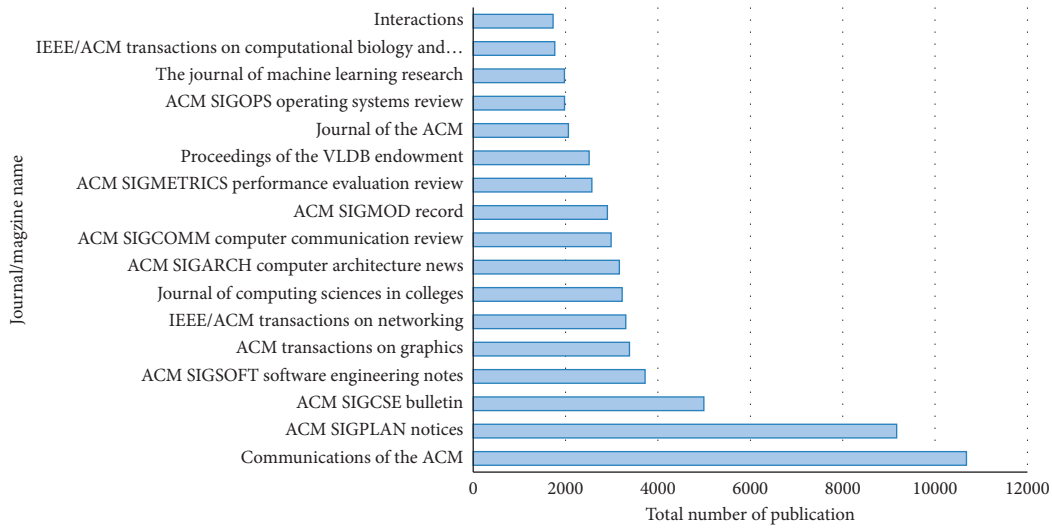

Figure 3: Magazine/Journal names and number of articles.

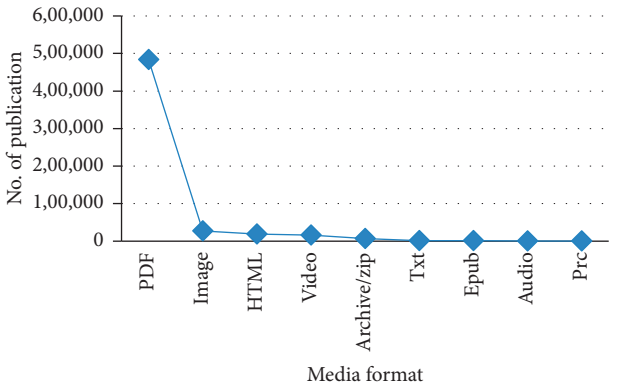

Figure 4: Total number of papers published along with the media forma.

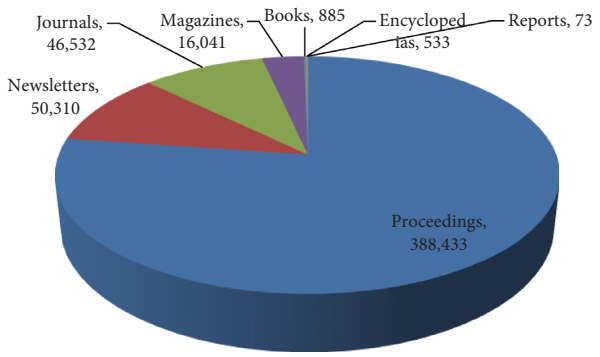

Figure 5: All publication and number of papers.

Table 1 shows some of the subdisciplines in which the papers are published along with the total number of publications.

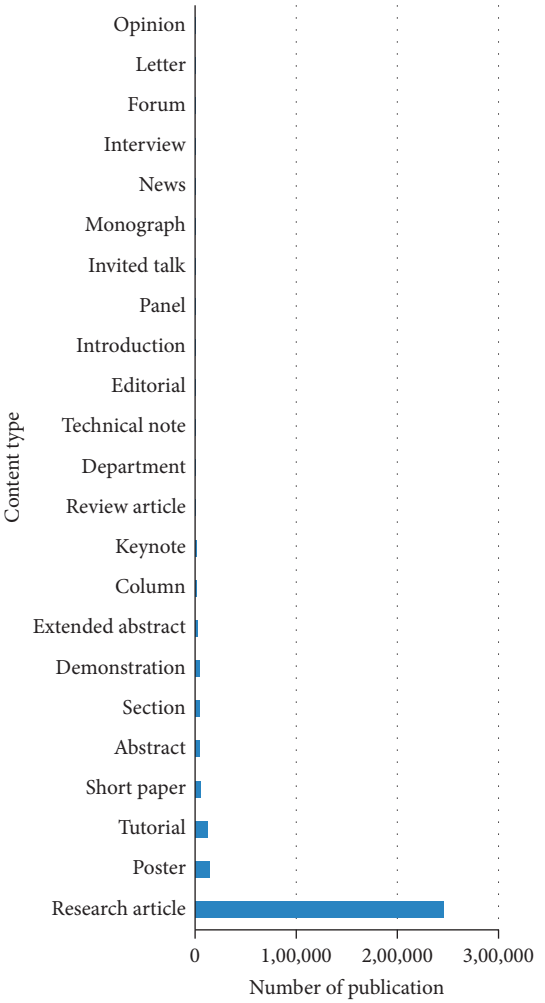

Figure 6: Content type and number of papers.

3.2. Rough Set Approach for Identification of Attack on Data Packets. ML algorithms are being in use for the identification of intrusion disturbing the organizations or its system [2, 6, 40–42]. In this paper, a rough set approach is used to identify the attack on data packets. The rough set approach works very well in situations of uncertainty by plotting the

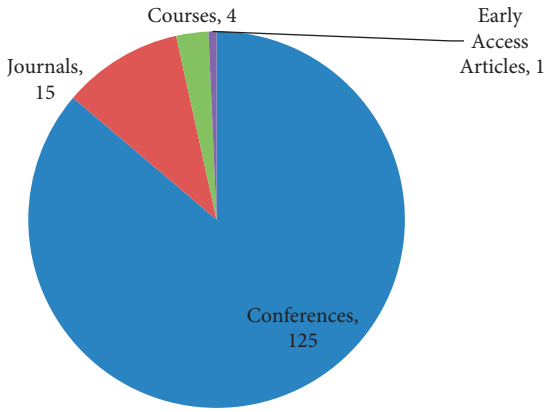

Figure 7: Content type and number of papers.

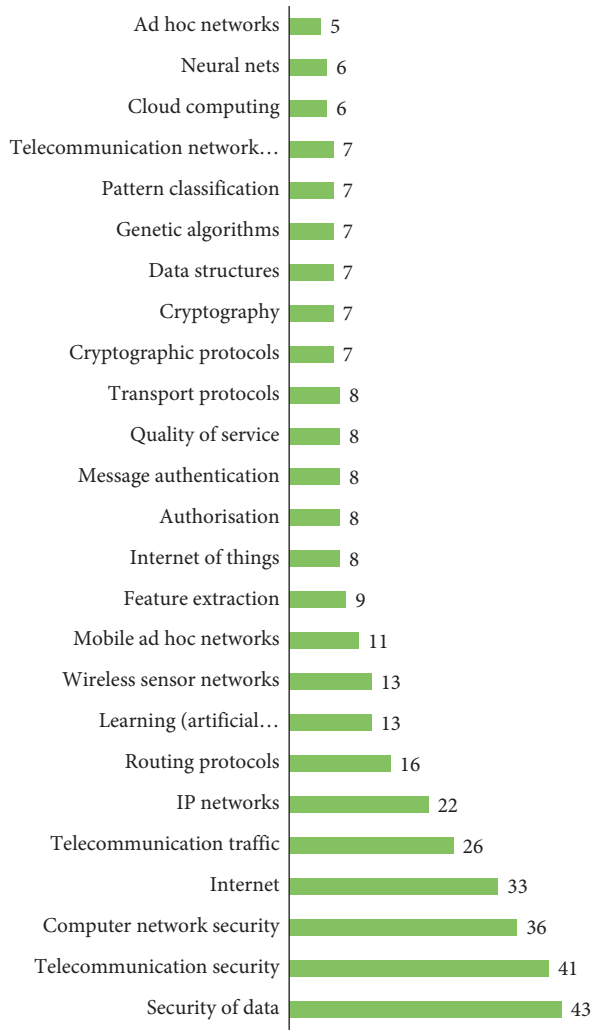

Figure 8: Content type and number of papers.

upper and lower approximations. The rough set approach is a combination of rules made up of associated features. The obtainable model consists of "IF THEN rules." The rough set was presented by Pawlak in 1982 [43]. It has specific lower

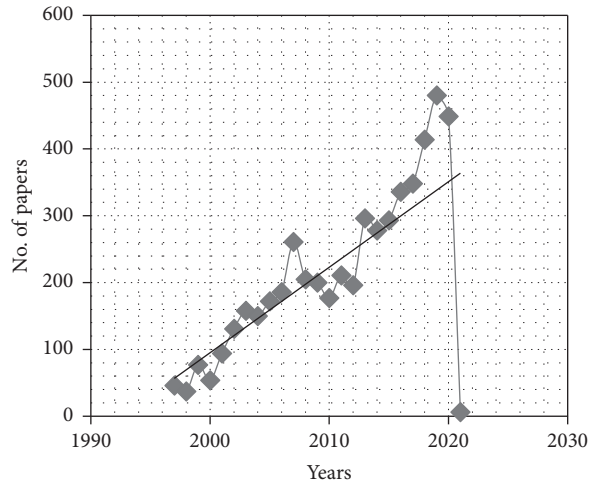

Figure 9: Content type and number of papers.

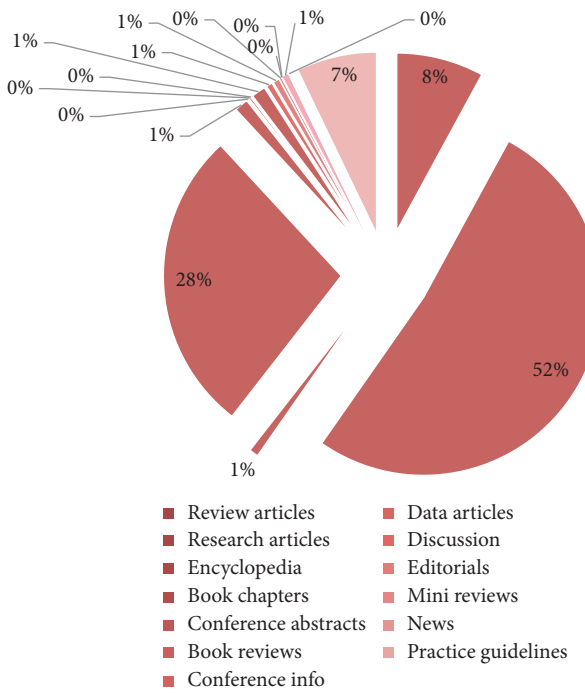

Figure 10: Content type and number of papers.

and upper approximation boundary areas. Rough sets can be mathematically presented as follows [44]:

$$\overline{BX} = \{x_i \in U | [x_i] \mathrm{Ind}(B) \cap x \neq 0\},$$
$$\underline{BX} = \{x_i \in U | [x_i] \mathrm{Ind}(B) \subset x\}. \quad (1)$$

Figure 14 presents the rough set concept.

Figure 15 presents the rough set theory workflow and its application. The main parts in the workflow are described in this section.

The above workflow of the proposed research has been implemented by the RSES software [45]. The library of RSES is

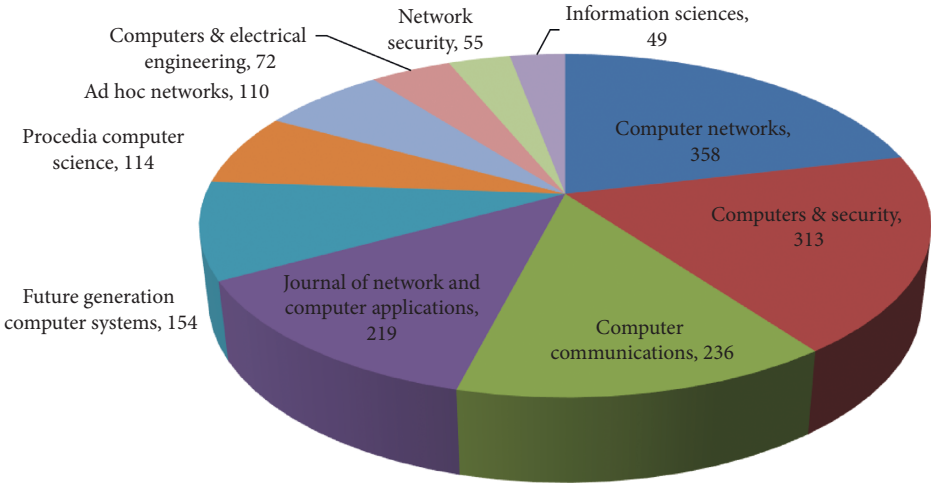

Figure 11: Content type and number of papers.

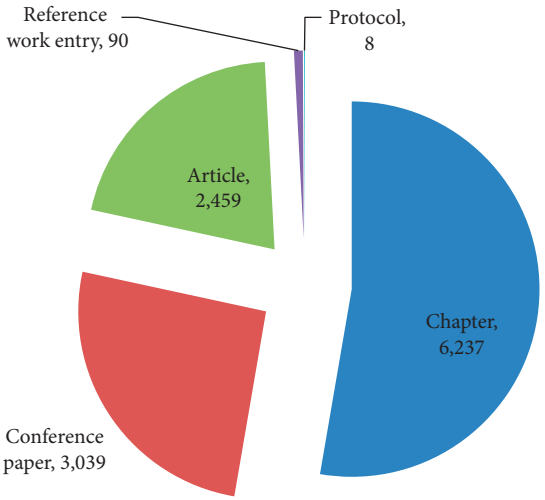

Figure 12: Content type and number of papers.

a well-known implementation of rough set theory process. The experimental process of the proposed study has followed the process that is common to use in rough sets for data analysis. Rough set and fuzzy rough set theories are based on some preliminary parts [46, 47]. The details are given as follows.

3.2.1. Indiscernibility Relation. The indiscernibility relation shows to which extent two objects are similar. In RST, if the information system (U, A) for any $B \subseteq A$, the equivalence relation R_B is defined by

$R_B(x, y) = \{(x, y) \in U^2 | \forall a \in B, a(x) = a(y)\}$, then x and y have the same values of the attributes in B, while in FRST the R is a fuzzy tolerance relation in U, where R satisfies

Reflexivity: $\forall x \in U, \quad R(x, x) = 1$

Symmetry: $\forall x, y \in U, \quad R(x, y) = R(y, x)$ τ – transitivity: $\forall x, y, z \in U, \quad \tau\ (R(x, y), R(y, z)) \leq R(x, z)$, where R is fuzzy t-equivalence relation.

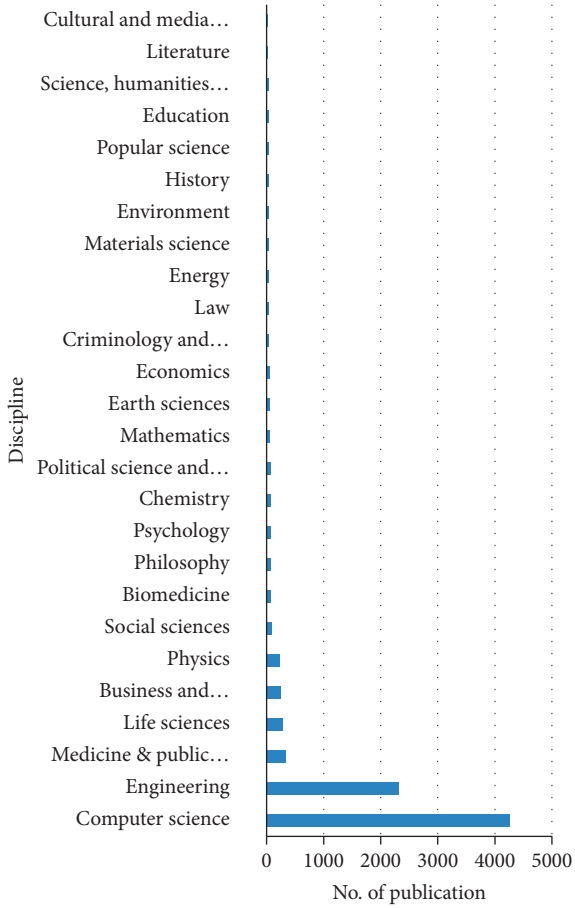

Figure 13: Content type and number of papers.

3.2.2. Approximations. The indiscernibility relation is used in the definition of lower and upper approximations. Given $B \subseteq A$, $X \subseteq U$ can be approximated using the information in B by constructing B-lower and B-upper approximations of X;

$$R_B \downarrow X = \{x \in U | [x]_B \subseteq X\},$$
$$R_B \uparrow X = \{x \in U | [x]_B \cap X \neq 0\}. \quad (2)$$

Table 1: Subdiscipline of publications.

Subdiscipline	Total no.
Computer communication networks	3,197
Cryptology	1,261
Computational intelligence	832
Computers and society	677
Information systems and communication service	627
Software engineering	541
Data structures and information theory	516
Operating systems	505
Robotics and automation	130
IT in business	412
Electrical engineering	373
Security	274
Theory of computation	270
Coding and information theory	256
Database management	252
Processor architectures	235
E-commerce/e-business	217
Image processing and computer vision	195
System performance and evaluation	193
Simulation and modelling	185
Legal aspects of computing	166
Circuits and systems	152
Programming languages, compilers, interpreters	145
Programming techniques	145
Computer applications	140
Pattern recognition	134
Robotics and automation	130
Control, robotics, mechatronics	128
Information systems applications (incl.Internet)	121
Engineering, general	115
Security science and technology	115
Health informatics	112
Computer appl. In administrative data processing	101
Computer engineering	87
Data storage representation	86
Electronics and microelectronics, instrumentation	81
Logics and meanings of programs	81
Public health	81
Medicine/public health, general	80
Probability theory and stochastic processes	78
Control and systems theory	76

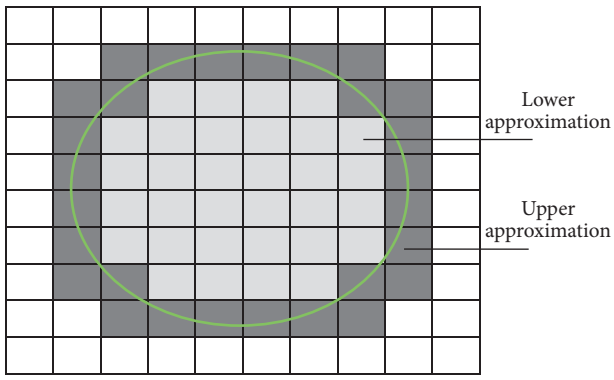

Figure 14: Concept of rough set.

In FRST, the following Radzikowska and Kerre crisp [48] lower and upper approximations are generalized by means of an implicator $\tau$and t-norm τ. Fuzzy indiscernibility relation R_a and a fuzzy set X in U:

$$\begin{aligned}(R_B{\downarrow}X)(y) &= \inf_{x\in U}\tau\left(R_B(x,y),X(x)\right),\\ (R_B{\uparrow}X)(y) &= \sup_{x\in U}\tau\left(R_B(x,y),X(x)\right).\end{aligned} \tag{3}$$

3.2.3. Regions and Degree of Dependency. In a decision system $(U, A\cup\{d\})$, the positive and boundary regions of $B\subseteq A$ can be defined in B-lower and B-upper approximations of the equivalence classes $[x]_d$.

The B-positive region

$$\mathrm{POS}_B = \cup_{x=U} R_B{\downarrow}[x]_d. \tag{4}$$

And the B-boundary region

$$\mathrm{BND}_B = \frac{\cup_{x=U} R_B{\uparrow}[x]_d}{\cup_{x=U} R_B{\downarrow}[x]_d}. \tag{5}$$

The degree of dependency of the decision attribute d on the set of conditional attributes B can be computed by

$$\gamma_B = \frac{|\mathrm{POS}_B|}{|U|}. \tag{6}$$

3.2.4. Discernibility Matrix. In RST, the information system (U, A) and the discernibility matrix $M(A)$ are a symmetric $n\times n$ matrix whose elements (C_{ij}) are defined as

$$C_{ij} = \left\{a\in A: a(x_i)\neq a(x_j)\right\} \text{ for } i,j = 1,\ldots,n. \tag{7}$$

In RST the discernibility matrix can be defined as

$$C_{ij} = \left\{\begin{array}{ll}\left\{a\in A: a(x_i)\neq a(x_j)\right\}, & \text{if } d(x_i)\neq d(x_j)\\ \theta, & \text{othewise,}\end{array}\right\}. \tag{8}$$

(1) Decision/Information Table. An information system is denoted as

IS = (U, A) where U is the universe of nonempty finite set, and A is attribute of nonfinite set.

(2) Indiscernibility, Reduct And Core. The indiscernibility relation IND (B) is defined as if IND (B) = IND $(B-\{a\})$, for IS = (U, A), for any subset of attributes $B\subseteq A$. Then, $a\in B$ is dispensable, otherwise indispensable in B, while set B can be called independent if all attributes are indiscernible. Reduct is a basic notion of rough set analysis. Reduct can be defined by indiscernibility relation, if $B\subset A$ and IND (b) = IND (B). Core is the intersection of all reducts. Core (B) = Red (B), where red (B) is all the reducts in B.

(3) Cut and Discretization. A Cut mostly appears in the context of discretization process. The discretization is a

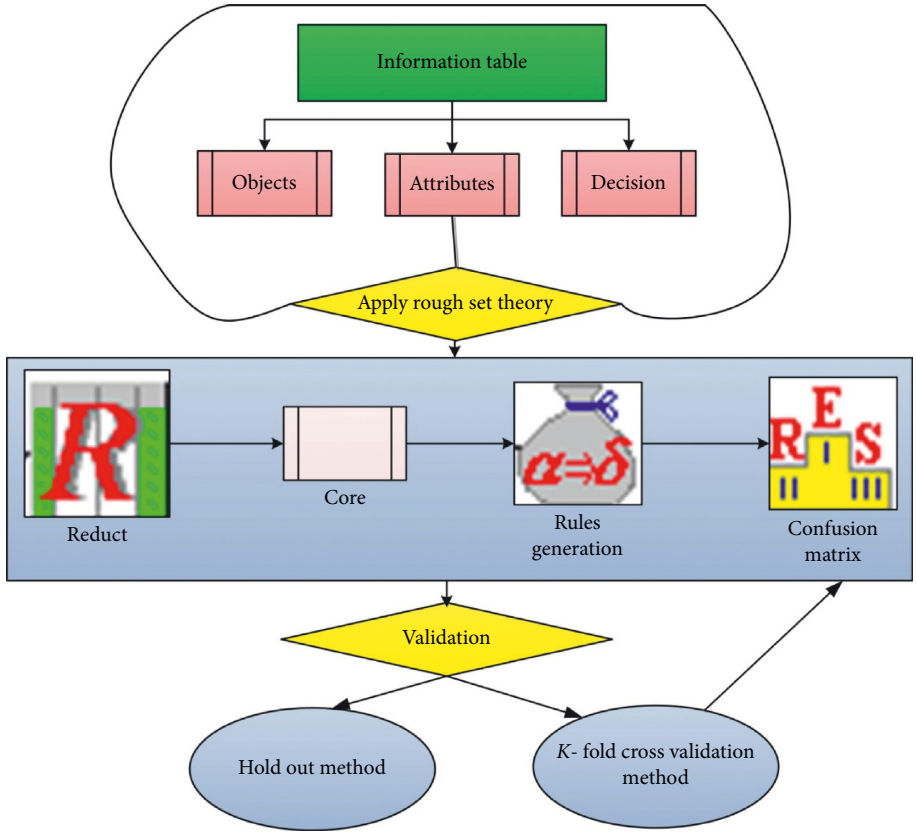

Figure 15: Generic rough set process.

process of grouping the data attributes for the calculation cuts and continuous variables, converting them into discrete attributes [49].

(4) Rules Generation. After constructing reduct sets, rules are generated in the form of (IF C THEN D), where "C" is the condition, and "D" is the decision value.

(5) Measurements for Classification. The formulation of measures is given as follows:

$$\begin{aligned}
\text{Sensitive measure (Recall)} &= \frac{TP}{P}, \text{ where } P \\
\text{Specificity} &= \frac{\text{TN}}{N} \geq 1 - \text{Specificity} \\
\text{Precision} &= \frac{\text{TP}}{\text{TP} + \text{FP}}, \\
\text{Accuracy} &= \frac{\text{TP} + \text{TN}}{\text{P} + \text{N}}, \\
\text{Coverage} &= \frac{\text{No of cases satisfying conditions and decision}}{\text{No of cases satisfying conditions}}.
\end{aligned} \tag{9}$$

4. Results and Discussions

The experimental study has used the dataset available at Kaggle "Attack Prediction on Data Packets" that was used in the proposed research. The experimental work was performed by the RSES software. The rough set approach consists of different algorithms such as Genetic algorithm, Exhaustive algorithm, Covering algorithm, and LEM2 algorithm. The experimental work has used the K-NN algorithm. The accuracy of the K-NN was 88% for the total

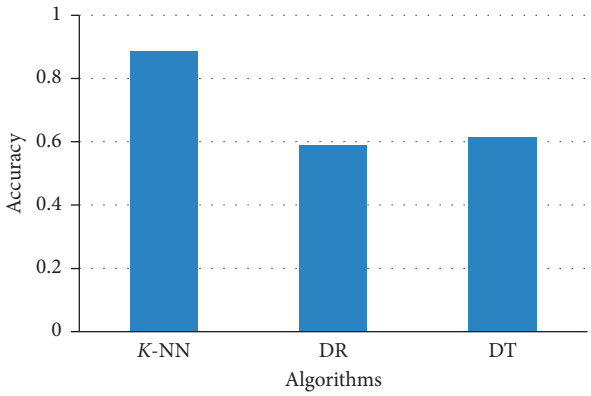

Figure 16: Overall comparison of algorithms for the proposed study.

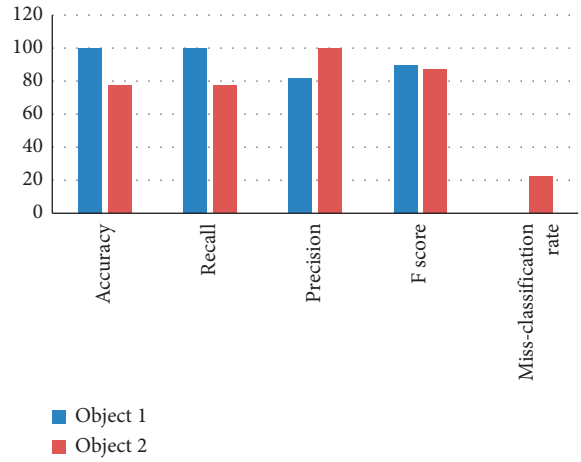

Figure 17: KNN based classification results.

objects of 8459. For cross validation purposes, the Decision rules and Decomposition tree algorithms were used. The DR algorithm shows accuracy of 59.1%, while the DT shows accuracy of 61.5%. The comparison of all these algorithms is shown in Figure 16.

After evaluating the proposed model for various parametric measures such as accuracy, F-measure, specificity, precision, recall, and miss-classification rate, it was concluded that the KNN performs very well among other classification algorithms as depicted in Figure 16. The other two generic algorithms, decision trees and decision rules, are used to check the applicability of the KNN-based recognition model. Figure 17 shows the experimental results of the KNN model.

(1) Decision trees–Figure 18 shows the recognition capabilities of the decision trees based model based on different performance measures.

(2) Decision rules–Figure 19 shows the recognition capabilities of the decision trees based model based on different performance measures.

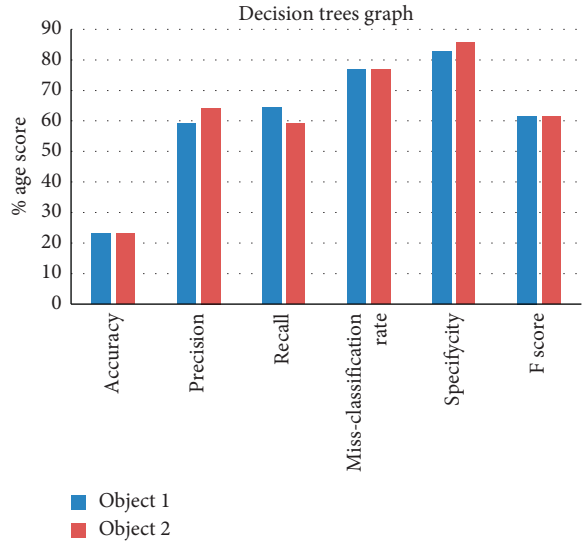

Figure 18: Decision trees based recognition model.

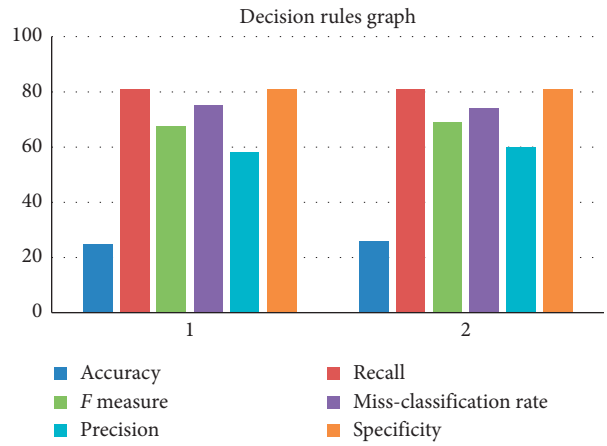

Figure 19: Decision rules recognition rates.

5. Conclusion

Information security is considered to be one of the important factors for any network and information communication. An organization or system of the organization with optimum security can lead to a successful business and can earn huge profit on the business they are doing. With the passage of time, the developments in information security are rising. Protecting the data and information inside the network becomes a challenging task for practitioners and researchers. To tackle such issues, an efficient and accurate mechanism is the dire need of modern day information industry. The proposed research presents the detection of data packets attack through the use of the rough set theory for security purposes of data packets and communication. The experimental work was performed by the RSES tool, and the results of the proposed study show that the research is capable of detecting data packets attack.

Data Availability

No data are available.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] H. H. Song, "Testing and evaluation system for cloud computing information security products," in *Proceedings of the 3rd International Conference on Mechatronics and Intelligent Robotics (ICMIR-2019)*, Yunnan, China, December 2020.

[2] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, Article ID 100227, 2020.

[3] J. Yuan and X. Luo, "Regional energy security performance evaluation in China using MTGS and SPA-TOPSIS," *Science of the Total Environment*, vol. 696, pp. 1–11, 2019.

[4] X. Wu, S. Liu, Y. Sun, Y. An, S. Dong, and G. Liu, "Ecological security evaluation based on entropy matter-element model: a case study of Kunming city, southwest China," *Ecological Indicators*, vol. 102, pp. 469–478, 2019.

[5] X. Wang, J. Li, X. Kuang, Y.-A. Tan, and J. Li, "The security of machine learning in an adversarial setting: a survey," *Journal of Parallel and Distributed Computing*, vol. 130, pp. 12–23, 2019.

[6] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," *Procedia Computer Science*, vol. 127, pp. 388–397, 2018.

[7] Z. Zhang, J. Wen, X. Wang, and C. Zhao, "A novel crowd evaluation method for security and trustworthiness of online social networks platforms based on signaling theory," *Journal of Computational Science*, vol. 26, pp. 468–477, 2017.

[8] Y. Cherdantseva, J. Hilton, O. Rana, and W. Ivins, "A multifaceted evaluation of the reference model of information assurance & security," *Computers and Security*, vol. 63, pp. 45–66, 2016.

[9] M. Jouini, L. B. A. Rabai, and R. Khedri, "A multidimensional approach towards a quantitative assessment of security threats," in *Proceedings of the Procedia Computer Science the 6th International Conference on Ambient Systems*, pp. 507–514, London, UK, December 2015.

[10] S. Nazir, S. Shahzad, M. Nazir, and H. U. Rehman, "Evaluating security of software components using analytic network process," in *Proceedings of the 11th International Conference on Frontiers of Information Technology (FIT)*, pp. 183–188, Islamabad, Pakistan, December 2013.

[11] Z. Gu, S. Nazir, C. Hong, and S. Khan, *Convolution Neural Network Based Higher Accurate Intrusion Identification System for the Network Security and Communication*, Security and Communication Networks, Plymouth, UK, 2020.

[12] X. Huang and S. Nazir, *Evaluating Security of Internet of Medical Things Using the Analytic Network Process Methods*, Security and Communication Networks, Plymouth, UK, 2020.

[13] M. Li, S. Nazir, H. U. Khan, S. Shahzad, and R. Amin, *Modelling Features-Based Birthmarks for Security of End-To-End Communication System*, Security and Communication Networks, Plymouth, UK, 2020.

[14] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[15] S. Nazir, S. Shahzad, S. Mahfooz, and M. N. Jan, "Fuzzy logic based decision support system for component security evaluation," *International Arab Journal of Information and Technology*, vol. 15, no. 2, pp. 1–9, 2018.

[16] H. U. Rahman, A. U. Rehman, S. Nazir, I. U. Rehman, and N. Uddin, "Privacy and Security—Limits of Personal Information to Minimize Loss of Privacy," *Lecture Notes in Networks and Systems,Advances in Information and Communication*, pp. 964–974, 2020.

[17] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, Article ID 152316, 2020.

[18] J. Zhang, S. Nazir, A. Huang, and A. Alharbi, *Multicriteria Decision and Machine Learning Algorithms for Component Security Evaluation*, Security and Communication Networks, Plymouth, UK, 2020.

[19] https://www.kaggle.com/vtu10547/attackedM. N. Shukla,.

[20] I. Kotenko and A. Chechulin, "Common framework for attack modeling and security evaluation in SIEM systems," in *Proceedings of the IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber*, Besancon, France, November 2012.

[21] P. Subsorn and S. Limwiriyakul, "A comparative analysis of internet banking security in Thailand: a customer perspective," *Procedia Engineering*, vol. 32, pp. 260–272, 2012.

[22] I. Kotenko and A. Chechulin, "Computer attack modeling and security evaluation based on attack graphs," in *Proceedings of the the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Berlin, Germany, September 2013.

[23] S. ManjiaTahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, 2020.

[24] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers and Security*, vol. 92, Article ID 101747, 2020.

[25] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin et al., "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, 2020.

[26] Fuzon, "Internet of medical things (IOMT): new era in healthcare industry," 2019, https://www.fuzon.io/insight/iomt-in-healthcare-industry.

[27] S. Elder, "87% of healthcare organizations will adopt Internet of Things Technology by 2019," 2019, https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712.

[28] A. ARAMPATZIS, "Protecting modern IoMT against cybersecurity challenges," https://www.tripwire.com/state-of-security/healthcare/modern-iomt-cybersecurity-challenges.

[29] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: taxonomy and risk assessment," in *Proceedings of the IEEE 42nd Conference on Local Computer Networks Workshops*, pp. 112–120, Singapore, October 2017.

[30] J. Rockoff, *J&J Warned Insulin Pump Vulnerable to Cyber Hacking*, Wall Street Journal [Internet], NY, USA, 2016.

[31] A. Mondal, P. Rao, and S. K. Madria, "Mobile computing, IoT and big data for urban informatics: challenges and opportunities," in *Handbook of Smart Cities*, pp. 81–113, Springer, Berlin, Germany, 2018.

[32] N. A. b. Mohd and Z. F. Zaaba, "A review of usability and security evaluation model of ecommerce website," in *Proceedings of the the Fifth Information Systems International Conference*, Surabaya, Indonesis, July 2019.
[33] W. Mao, Z. Cai, D. Towsley, Q. Feng, and X. Guan, "Security importance assessment for system objects and malware detection," *Computers and Security*, vol. 68, pp. 47–68, 2017.
[34] S. Khan, H. Ali, Z. Ullah, N. Minallah, S. Maqsood, and A. Hafeez, "KNN and ANN-based recognition of handwritten Pashto letters using zoning features," *International Journal Of Advanced Computer Science And Applications*, vol. 9, no. 10, pp. 570–577, 2018.
[35] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE Transactions on Signal Processing*, vol. 45, no. 11, pp. 2673–2681, 1997.
[36] A. Graves and J. Schmidhuber, "Framewise phoneme classification with bidirectional LSTM and other neural network architectures," *Neural Networks*, vol. 18, no. 5-6, pp. 602–610, 2005.
[37] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, *Enforcing Security in Internet of Things Frameworks: A Systematic Literature Review*, Internet of Things, vol. 6, Article ID 100050, 2019.
[38] J. Ahamed and A. V. Rajan, "Internet of things (IoT): application systems and security vulnerabilities," in *Proceedings of the 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, pp. 1–5, Ras Al Khaimah, UAE, December 2016.
[39] C. Hosmer, "IoT vulnerabilities," in *Defending IoT Infrastructures with the Raspberry Pi: Monitoring and Detecting Nefarious Behavior in Real Time*, pp. 1–15, Apress, Berkeley, CA, USA, 2018.
[40] Z. Katzir and Y. Elovici, "Quantifying the resilience of machine learning classifiers used for cyber security," *Expert Systems with Applications*, vol. 92, pp. 419–429, 2018.
[41] M. Belouch, S. El Hadaj, and M. Idhammad, "Performance evaluation of intrusion detection based on machine learning using Apache Spark," *Procedia Computer Science*, vol. 127, pp. 1–6, 2018.
[42] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.
[43] Z. A. Pawlak, "Rough sets," *International Journal of Computer & Information Sciences*, vol. 11, no. 5, pp. 341–356, 1982.
[44] Z. Pawlak, *Rough Set: Theoretical Aspects of Reasoning about Data*, Kluwer Academic Publishers, Norwell, MA, USA, 1992.
[45] RSES2, http://www.mimuw.edu.pl/%7Eszczuka/rses/start.html.
[46] L. S. Riza, A. Janusz, C. Bergmeir et al., "Implementing algorithms of rough set theory and fuzzy rough set theory in the R package "RoughSets"" *Information Sciences*, vol. 287, pp. 68–89, 2014.
[47] S. Nazir, S. Shahzad, and L. S. Riza, "Birthmark-based software classification using rough sets," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 859–871, 2016.
[48] A. M. Radzikowska and E. E. Kerre, "A comparative study of fuzzy rough sets," *Fuzzy Sets and Systems*, vol. 126, no. 2, pp. 137–155, 2002.
[49] J. G. Bazan and M. Szczuka, "The rough set exploration system," *Transactions on Rough Sets III*, pp. 37–56, 2005.