REPUBLIC OF TÜRKİYE
ALTINBAŞ UNIVERSITY
Institute of Graduate Studies
Information Technology

A NEW DEEP LEARNING-BASED FRAMEWORK FOR CYBERSCURITY PROBLEMS

Hanan Basim Naje KERMASHA

Master's Thesis

Supervisor

Asst.Prof. Dr. Abdullahi Abdu Ibrahim

Istanbul, 2022

A NEW DEEP LEARNİNG-BASED FRAMEWORK FOR CYBERSECURİTY PROBLEMS

Hanan Basim Naje KERMASHA

Information Technology

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled A NEW DEEP LEARNING-BASED FRAMEWORK FOR CYBERSECURITY PROBLEMS" prepared HANAN BASIM NAJE KERMASHA and submitted on 13/12/2022 has been **accepted unanimously** for the degree of Master of Science in INFORMATION TECHNOLOGIES.

_____

Asst.Prof. Dr. Abdullahi Abdu IBRAHIM
Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Engineering and Architecture, Altinbaş University	_____
Asst. Prof. Dr Ayça Kurnaz TÜRKBEN	Department of Computer Engineering,and Architecture, Altinbaş University	_____
Asst. Prof. Dr. Serdar KARGIN	Department of Engineering and Architecture, Beykent University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis

Submission date of the thesis to the Graduate Education Institute: ____/____/____

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Hanan Basim Naje KERMASHA

Signature

DEDICATION

For those who taught me that the world is a struggle, and its weapon is knowledge, my dear father. To the most wonderful woman in existence, my dear mother to my companion, my beloved husband, my wonderful brothers and children, and everyone who has supported me in my academic career.

I dedicate this success

PREFACE

I would like to thank my supervisor Asst.Prof. Dr. Abdullahi Abdu Ibrahim and my all family.

ABSTRACT

A NEW DEEP LEARNING-BASED FRAMEWORK FOR CYBERSCURITY PROBLEMS

KERMASHA Hanan Basim Naje

MSc, Information Tecnology Istanbul Altınbaş University,

Supervisor: Asst.Prof. Dr. Abdullahi Abdu IBRAHİM

Date: December /2022

Pages: 68

In this study, we proposes new study based CNN-GA-random forest to detect the SQL injection attacks in IoTs. In the first stage, the CNN applied to extract high level features from input SQL inquiries. Then, the output of the CNN wired to the random forest. The random forest is robust classifier used in several classification and regression problems and presented remarkable results when compared with other classifiers. Then, the genetic algorithm applied to train the CNN to select best weight and basis of the model. The genetic algorithm is robust optimization algorithm and used in several fields to enhance the performance of the models such as design, classification, regression and estimation. The proposed system showed results with an accuracy of 99.93% compared to some studies.

Keywords: CNN, Cybersecurity, SQL Injection, Genetic Algorithm.

TABLE OF CONTENTS

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

SVM : Support vector machine

NN : Neural Network

RBF : Radial Basis Function

ANN : Artificial-Neural-Network

CNN : Convolutional neural network

1. INTRODUCTION

Cyber security is a concept that emerged as a result of the widespread use of the Internet and the rapid digitalization of daily data communication. The widespread opening of the Internet for civilian use in 1991 and the developing computer technology added the digital and virtual environment to the connections of individuals in the physical world. This field, which we call 'cyber space' nowadays, has effectively entered our lives with the developing telecommunication technology in the 2000s [1,2]. The increase in the prevalence of communication technologies has also encouraged the production of digital data. It is now on the agenda to use the data of not only institutions, companies, political structure and economic elements, but also individuals (citizens) who form the basis of them. The concept of cyber security, which is being used frequently today, in its most basic sense, is a definition that deals with security problems in the field of cyberspace. Cyber security, in its simplest sense, is based on the protection of cyberspace from all kinds of threats. It is a holistic and compiling concept. It is a unifying element that encompasses all layers, from the smallest cybercrime to the largest and most complex attack. From the perspective of international relations, the principle that the state should protect the individual is also essential here. However, it should be underlined that there are huge differences between the definition that was used as a basis for the use of this concept in the 1990s and the dynamics in the field and today's factors. Cybersecurity based on cyberspace is not a virtual space per se. Cyberspace is a space consisting of the interaction of physical and virtual space. The interaction of both areas makes the concept of cyber security even more important. If transactions in the virtual space did not have an impact on the physical world, we would probably not be talking about cybersecurity. In other words, the concept of cyber security emerges because attacks or moves in the cyber space have an effect in the physical space. Therefore, the terminology used in the field of cyber security is necessarily based on the concepts of national security.

1.1 CONTRIBUTIONS

This study presented several contributions related to cybersecurity filed:

i. The deep learning model CNN combined with the optimization algorithm known as genetic algorithm to select best weight and basis.

ii. The proposed method is new cybersecurity problems based on SQL injection.

iii. The obtained results compared with several traditional techniques and show that the proposed method is best.

2. OVERVIEW

2.1 CYBERSECURITY

These security threats arising from information and technology have necessitated re-examination of all aspects of security. Although these threats are called new, they already existed before. However, the fact that the political atmosphere of the Cold War period made one think of security on a purely military basis and that the effective speed and impact of technological globalization was not felt as in the 21st century prevented these new threats from gaining much space in the perception of security. However, in the 21st century, the new phases that information-based technologies have reached through the rapid and sharp changes they have undergone have created different and new security problems for states, private institutions and individuals who carry out their administrative and financial affairs in the computer environment. In previous periods, this area, which expresses the spatial and spatial environment formed by electronic communication networks between people at different computer terminals and was handled with a metaphorical reductionism, was called cyberspace, but it is used with all the tools of information, communication and technology in terms of security in a wide range, both theoretically and conceptually. it has spread to the area. 45 On the other hand, as stated, individuals and states becoming dependent on this field by taking advantage of the rapidity and ease of information and technological developments have brought along threats and risks originating from cyberspace, which is not costly but has a high damaging effect. Because the greatest benefit of cyberspace in terms of possibilities and capacities has been to terrorist and criminal groups as non-state actors, but also to individual criminals. Because classical warfare tools, which were previously owned only by states, were tools that non-state groups and individuals could not have due to the cost burden. However, the physical limitations and irregularities of cyberspace provide convenience for these groups to carry out their targeted actions in this environment. Failure to provide information and technology security for states in an environment where only a computer or a mobile phone would be sufficient for terrorist groups to carry out the action can harbor serious problems for national security. At this point, while information and technology-oriented discoveries create security threats arising from the relations between states, in addition to the benefits and gains they provide to states, on the other hand, trans-state groups can pose a security threat to states. In this direction, states have begun to think of classical

security tools not only as military-oriented, but also information-oriented, through information technology. Moreover, they have also tried to transform the forms of warfare conducted in the digital environment, such as attack, defense and intelligence, based on information technology, into military capabilities [3]. The superiority achieved in information technology will also enable states to determine the form, method and nature of wars in the struggles to be made in cyberspace. Therefore, it is seen that developments in information and communication technologies increase cyber security threats.

The development, access and availability of production based on information technology takes place in cyberspace. Since the sharing and use of information in electronic media in cyberspace can be open to everyone, it is also observed that information, which has become an important power in its own right, may be exposed to some dangers. In other words, while the enormous revolutions in technology in the new world order of the 21st century will present favorable opportunities for states in terms of power, they will also bring along new dangers and risks that will preoccupy the minds of states. This situation gives a new perspective to the notion of security of information systems, and in direct proportion to this, it makes it essential for states to ensure the security of cyberspace, where information systems come to life. Because for the states that transfer their military, economic, social and political work to the cyber environment, this area is included in the scope of national security. In this framework, cyberspace includes not monolithic military elements but also economic, political and social elements within the scope of national security of states [4]. Although there were attacks originating from the cyber world during the Cold War period, it is seen that the main impact and violence of cyber attacks are experienced after the 21st century. Experienced examples of cyber attacks such as Israel's Orchard operation against Syria, Russia's cyber attacks against Georgia in the 8.8.8 war, and the 2010 Stuxnet attacks on Iran's nuclear production centers are examples of cyber attacks, threats, wars and wars. showed that the dangers cannot be ignored. It is accepted by the states that when the word cyber is added in front of the attacks originating from certain physical limitations and an environment devoid of laws, terrorism and war, the views and perceptions of cyberspace turn into a realm of reality rather than a metaphorical abstraction (Owens et al., 2009; Zhang, 2008). 2012). If states accept survival and national security as primary goals in the anarchic environment of the international system, they should tend to see cyberspace, which contains opportunities for economic, military, political and social areas, as well as serious threats, as

an inseparable part of the scope of national security. Because the notion of national security has become important within the scope of security since it presents integrity with all its economic, political, military and political dimensions and poses a threat to the security of all these elements in cyberspace. Thus, the new technological tools that states and non-state groups, whose dependence on information technologies are increasing day by day, have begun to use in operations, intelligence and wars contribute to the rethinking process in their perceptions and fields of security threats. As it is observed, it is seen that the development of technology and the understanding of order that it creates with it, dialectically clustered cyber threats based on information and communication technologies, again emerged with tools and methods based on information and communication technologies. Therefore, states that actively use cyberspace-based technological tools have tried to take precautions against threats to their national security from this area, especially by developing systematic methods related to cyber attack and defense.

2.2 CYBER SECURITY AND RELATED CONCEPTUAL FRAMEWORK

The universalized structure of cyber networks that transcends national borders and cannot be physically limited should now be included in international relations in terms of cyber security threats. This situation also constitutes the subject of other studies that can be divided into many sub-branches. The facts of cyber terrorism, threat and war, which are the practical forms of security threats in the cyber environment, will be discussed within the content of the aforementioned sub-branches. Cyber security was first used by computer engineers in the 1990s to express security problems related to networked computers, but when developments emerged that revealed that these security problems could have devastating social consequences, they became a major threat to the western world over time by politicians, private companies and the media. evaluated as “Electronic Pearl Harbors”. The events of September 11, information technologies, computers focused on security, especially the protection of information technology infrastructures, electronic surveillance, terrorists' use of the internet as a communication tool [5]. The basic attack tools that pose a threat to cyber security over networks are also different due to the unique nature of the environment. Spyware over networks, eavesdropping on network traffic, 48 manipulative baiting, spam e-mails, denial of service, worms and bootnets meaning slave computer are the attack tools in the cyber environment. At this point, Joseph Nye classified the main threats to the cyber

security of states as cyber threats created by states against each other and threats to the cyber security of states by non-state actors. According to this classification, cyber wars and economic-based espionage and intelligence threats are mostly associated with states, while crimes committed through cyber networks and cyber terrorism are associated with non-state actors. The increasing importance of the cyber environment in the eyes of all actors, with its differentiating aspects such as cyber threat, cyber war, cyber terrorism, and the concepts that are the expression of the unknown dangers from where and how they will come into the dictionary of security. So much so that, after the cyber-attacks against NATO, the collective defense organization of Western countries, especially its member Estonia, the cyber environment was accepted as an asymmetrical threat-creating area of action, and subsequently the Cooperative Cyber Defense Center of Excellence (CCD COE) was established in 2008. In addition, in the declaration published after the Bucharest Summit in 2008, NATO declared that it will continue its determination to strengthen the information systems of its members against cyber-attacks, as well as ensured the adoption of the cyber defense policy at the summit and decided to establish structures that will develop it and authorities to realize it. In addition, it was emphasized that the basis of NATO's cyber security policy is defense. Of course, the increasing impact of attacks originating from the cyber environment, with its different dimensions, has become conjugated with power, and as a result, having the ability to carry out cyber warfare by including network-supported capabilities and starting points with the intention of keeping dominance of this environment, national-oriented modern armies and international organizations such as NATO. has been the main goal for organizations. In this context, NATO has increased its cyber attack capacity by adding offensive units to the defense units it has built within the scope of cyber security. In this respect, NATO, which considers the transformation of traditional security understanding and tools necessary, has included military concepts such as network-supported combat and operation, impact-oriented operation, information-based warfare and operation, and has started the Network Supported Capability Program in various countries in order to perform these capabilities. In the new conjuncture of the 21st century, it is of primary importance for states to adapt to the technological developments produced by the cyber environment when observing from the national security framework (Huhtinen and Laitinen, 2012: 65-80). Because, at the beginning of the measures to be taken against the threats created by using tools originating from the cyber environment, the use and knowledge

of these tools comes first. For this reason, if a state's policy consists of measures taken to protect the security of the country's diplomatic decisions, especially the secrets related to the privacy of the country, in this case, the non-military means of combating these non-military threats in the classical sense make non-military tools essential. The information age offered by the cyber environment, which has become an important power component in the 21st century, has also transformed socio-economic, political and military institutions. For this reason, factors such as the division, dissemination and preservation of information, in addition to the collapse of the information-based systems of the opposing states, the ability to see the depth of the enemy, mobility, flexibility and lightness, are gathered under the same roof and care is taken to ensure that they are all together in both the organizational structure and the weapon equipment systems. [7]. In this case, it will naturally speed up the countries to revise their military structures. Because from now on, in the 21st century, states will use knowledge and technology-based science as an encouraging element for more powerful and effective military units and equipment. However, rapid and effective information-based transformations have brought to light new and different security threats, as well as the military structures of states, and have also increased the dimensions of the existing classical threats [8] . In this direction, since each state must determine its information elements according to its own political, geographical, military, socio-political and economic form, and develop and use information systems appropriate for these information elements, 50 strategies must be created [9] made it necessary to add the cyberspace dimension of security in the security literature. Because the technological developments derived from the cyber environment do not have a static structure, on the contrary, they become more visible with their dimensions and effects with each passing day, and since the threats will increase at the same rate, the security dimension of cyber is beginning to be voiced among the serious threats against national security. The complex and multidimensional unique environment of cyberspace, which is described as the fifth dimension after air, sea, space and land, has made it one of the priority security areas of the notion of cyber security. Cyber security, which is defined as the protection of all kinds of information in the cyber environment, is also related to the production, storage, functionalization and transmission of information. In this context, in the most general sense, cyber security is used to protect the assets of institutions, organizations and users in the cyber environment; tools, policies, security concepts, risk management approaches, activities, trainings, and best practices and technologies [10]. In

order for this new dimension of security to reach its ultimate goal, some security criteria and qualifications must be provided or found in the cyber environment. These; confidentiality, authenticity, accuracy and integrity, consistency, reliability, continuity, accessibility and measurability [11]. Considering the information-based systems used at the level of states and the damage and vulnerability of their assets as a result of attacks derived from counter-information systems, the chaos environment to be experienced will put the states in a difficult situation. For example, the cyber attack that took place in Estonia in 2007 revealed how vulnerable a country's critical infrastructures can be to threats from the internet. The reason why this threat is perceived as vital for Estonia is that many activities related to the public and private sectors in the country are carried out over the internet. Again, in Australia, an angry worker manipulated computer systems and released wastewater into rivers and parks, the disruption of the electricity system that killed 11 people in the USA and left 50 million people helpless through software 51, and the Stuxnet attack against Iran's nuclear facilities. attacks are among the examples that come to mind. Therefore, it is also important to protect critical infrastructure systems that are integrated with cyberspace and can be accessed over networks from attacks that may be faced, considering that they are important for the national security of states.

Critical infrastructures, which are defined as infrastructures containing information systems that can cause loss of life, large-scale economic damage, national security deficits or destruction of public order, when the confidentiality, integrity or accessibility of the information they process is impaired, are therefore included in the "National Cyber Security Strategy and Action Plans" documents of countries. has earned its place at the top. These documents, which are called Strategy and Action Plans in the world, cover the 2016-2019 period and aim to minimize existing risks in the light of certain principles, with general lines of strategic objectives;

i. Establishing a national critical infrastructure inventory, meeting the security requirements of critical infrastructures and auditing these critical infrastructures by the regulatory bodies (Annex-B) and creating legislation in line with international standards, including the audit approach in the field of cyber security.

ii. Sector regulatory agency, ministry, etc. Developing organizations' awareness and competencies in regulation and supervision within the scope of cyber security, and

making arrangements to protect organizations' information systems not only from attacks, but also from user errors and disasters.

iii. It is important for each institution to reach the competence to run its own information security management process and to raise the awareness of corporate managers on cyber security. In addition, it is important to emphasize the training of competent personnel in the field of cyber security and the encouragement of personnel, researchers and students who want to specialize in this field.

iv. Creating awareness of cyber security in every part of the society, carrying out awareness studies in the written and visual media in addition to the studies of educational institutions. 5. Providing legislative support to increase the effectiveness of institutional and sectoral SOMEs (Cyber Incidents Response Team) (Annex-C), making financial arrangements, meeting the need for competent personnel, providing information infrastructure and developing information sharing within the scope of the national cyber incident response organization.

v. With the aim of establishing a strong central public authority that will ensure coordination in the field of cyber security and the participation and coordination of public institutions, private sector, NGOs (Non-Governmental Organization), supervisory institutions, universities, developer companies and all other stakeholders, the national cyber security eco- creation of the system.

vi. Vulnerability analysis and certification in order to disseminate good examples within the National Cyber security ecosystem, to provide consultancy services, to share vulnerability, threats and useful applications, as well as to prevent the abuse of vulnerabilities contained in domestic or foreign hardware and software products used at critical points of information systems. doing the work. 8. Establishing a culture of secure software development and supply management. Developing domestic products by giving importance to R&D activities in order to reduce foreign dependency in cyber security.

vii. It has been framed as the development of national proactive cyber defense capability to eliminate threat elements before they attack, and the dissemination of effective

record management and IPv6 (Internet Protocol version 6) technologies to eliminate anonymity, which is the biggest advantage of threat elements in cyberspace.

In our globalizing world in the 21st century, the security of critical infrastructures and the uninterrupted maintenance of critical infrastructure systems on a 24/7 basis are of vital importance in ensuring the economic development and social welfare of the modern state. Although critical infrastructures vary from country to country; sectors such as banking, energy, information and communication, electronic communications, health and basic public services and their infrastructures are considered as critical infrastructure elements53 and these infrastructures are considered within the scope of strategic systems that should be protected at the national level since they are exposed to various civil and military threats [12]. In parallel, critical infrastructure components, which he defines as assets, systems and services, which, if damaged or destroyed in the EU, could have a serious negative impact on the vital social functions, health, safety, security, social welfare of the citizens and the effective functioning of the member states; energy, information and communication technologies, water, food, health, finance, public-law order and security, civil administration, transportation. Critical infrastructure components in the USA, which define vital critical infrastructures in the USA as physical or virtual systems and assets that, in the event of insufficiency or disappearance, have an adverse effect on security, national economic security, national public health and safety, or any combination of these elements; commercial facilities, communication, dams, defense industry, energy, finance, food and agriculture, information technology, nuclear, government administration facilities (Homeland Security, n.d.). As observed, it is seen that all of the critical infrastructure classifications and components are dependent on information systems and therefore controlled by information systems. This, in turn, has brought these infrastructures, which maintain their functionality with software-based systems, to a component of cyberspace, as well as the concept of cyber security, which will erode the classical security understanding, especially with its differing threat dimensions. According to Ünver and Canbay, who classify the layers of cyber security as Application Security, Service Security and Infrastructure Security, and their scope and dimensions as access control, authentication, data privacy, communication security, data integrity, accessibility and the privacy of states, these layers and the dimensions they produce Threats and attacks aimed at destroying, damaging, deleting, disclosing and preventing determine the content of cyber security (Ünver et al.,

2009: 3). In other words, the main objectives of cyber security are to provide confidentiality, integrity, accessibility, undeniability and privacy. In this, the key factor of cyber security is to ensure the information, but to ensure the accessibility of the information (the state of being accessible, ready to use and functional when needed in response to unexpected events and attacks), integrity (to ensure the data integrity of critical infrastructures against the accuracy of the transferred and shared data). It is the case of storing data transmitted, received or stored in information systems without defect or manipulation, confidentiality (communication carried out over information systems and the protection of confidential data of communication. It is to protect the privacy of states during the transmission of all important and sensitive data, and to protect the privacy of states during communication.). In this context, cyber security, which aims to protect its knowledge and qualifications, aims to minimize security vulnerabilities arising from information systems together with cyber threats and attacks. In the light of these issues, the increase in the possibility of cyber threats against countries, especially their critical infrastructures, and their coming to a point that will affect public order and security with great financial losses, required the issue to be handled by both national, regional and international institutions and organizations. Cyber security studies, which started in the late 1990s, have increased rapidly in recent years (Ünver, 2009). The studies carried out at the point of providing cyber security include important elements of cyber security studies; national policy and a cyber security strategy prepared within the framework of this policy, cyber threats and attacks, which usually affect life and property, are likely to result, defining and punishing these results and the actions and methods that lead to these results as crimes, especially cyber-attackers. deterrence is of great importance. Considering that the means and methods of cyber attacks have changed in parallel with technological developments, a legal framework should be established in this regard, since it is necessary to review the country's legislation and to eliminate the deficiencies, if any, regarding both the substantive and procedural aspects. In addition to the development of technical measures to increase the quality of software, hardware and business processes and make them safer, determining the institutional structuring on cyber security issues, Ensuring cooperation and coordination on a national basis and developing capacity, increasing awareness, Ensuring international cooperation and harmony are important in ensuring cyber security. elements stand out.

2.2.1 Cyber Space

The concept of cyberspace, which emerged from the field of science fiction in the 1980s and translated into Turkish as cyber space, cyber space and cyber space, has shown a remarkable development conceptually in the 21st century. While cyberspace, which follows a developmental course in parallel with the development of the internet and other information and communication technologies, emerges as a new area of conflict and conflict in the 21st century, which is called the new world order, in the wider social plane, including all the systems of the economy, it is the information and information layer. Although the use of communication tools such as telegraph and radio in the field of communication is more ancient, the computer and the internet, which were used by the state and then, thanks to its development in time, have led to the focus on the concept of cyber space. From a historical perspective, access and participation in cyberspace also limited the effectiveness of many actors in this environment due to the complexity of the field (Leiner et al., n.d.). On the other hand, after the 21st century, access and participation in the activity areas of cyber space have become available to states and people around the world. Today, approximately 2 billion people in the world can easily access the Internet, while there are more than 30 trillion individual web pages [13]. In particular, the rapid and effective rise of computers and the internet, it is observed that cyber space contains opportunities and threats both for and against, like a double-edged knife before political and social formations. This aspect not only increased the curiosity about the nature of the concept, but also the frequent use of the concept in the international environment, as well as the recent cyberspace-based attacks and the threats and risks in direct proportion to it. However, although this area has been taken seriously due to the high level of concerns and concerns about cyberspace in recent years, it has also been difficult to define since this area has its own dimensions within the framework of security risks. For example, the US Department of Defense, which made the first serious moves at the state level on cyberspace and established the defense wing called USCYBERCOM (United States Cyber Command), has made various definitions until recently [14]. Again, as can be observed from the definitions in the literary literature, which are tried to be made in detail in the following statements, there is no consensus on what exactly cyber space is, whether it is a manifestation of a physical space or a virtual space, and what it contains/contains. However, the only point that needs to be known about the notion of cyber space and on which a consensus has been reached is that the second suffix

of the concept, namely the space-space suffix, is not space in the sense of the void that corresponds to the infinity known in perceptions. Because cyberspace is primarily a human-made structure. It is the person who establishes and maintains the information environment produced, shared and collected in this field. Again, of course, human is the agent of multidimensional and functional analyzes of the use and orientation of digital tools, which are indispensable for the notion of cyberspace to find some kind of profit [15]. In other words, cyberspace is in a position beyond the virtual world, as it was once attributed, because it contains physical infrastructures such as information storage, sharing and dissemination via networks, along with the information environment, especially critical infrastructures, through human communities [16]. For this reason, cyberspace and the physical layer have become a whole. Because cyberspace, which goes beyond representing the three-dimensional space based on science fiction as in the times when it emerged, has constantly evolved with its concepts, tools and effects parallel to the development of informatics and technologies. Therefore, cyberspace, with its dimensions and effects, has a certain physical infrastructure and at the same time affects certain geographies, it is closer to the physical environment than a virtual platform [17]. When the etymology of the concept is examined, it is seen that it is far from the semantics that has been defined and gained meaning recently, and that it is derived from a different field. The expression cyber was pronounced during the ancient Greek civilizations. In 1948, the concept of Cybernetics, which was conceived by the mathematician Norbert Weiner as a discipline examining the control and communication discipline between animals and machines, was revived and detailed. The prefix cyber word means computer and electronics-based technologies. Here, the concept of cyberspace is a concept formed by the combination of the first phrase of the word cybernetics and the word space. The architect of this structuring of the concept and its use close to its meaning in today's semantics is William Gibson. While Gibson interpreted the concept of cyberspace as a technical field containing complex variables in the short story he published in 1982, in his novel Neuromancer in 1984, he defined it as a graphical platform that is difficult to visualize and contains enormous complexity of messages transferred by billions of networks in a more comprehensive and technical orientation. defined. The fact that the concept gradually felt its effect and practice with the development of information and technologies has also transformed the principles and dimensions of its definition. The effect of the dimensions of cyber space has not only found its place in technical dimensions, but also in political and

social layers. Cyberspace, which was once used only for communication purposes, has become to include many more critical infrastructures from the banking sector, such as transportation, communication, health and energy facilities, after the 21st century. In addition, SCADA (Supervisory Control and Data Acquisition) to provide command and control of the aforementioned sectors through surveillance control and data collection is provided by computer technologies of cyberspace, which also has physical infrastructures [18]. Thus, the developments in cyberspace technologies, which already have a complex technical system, and the associated increases in their use, have allowed to lay the groundwork for changes in the political and social field. For this reason, in every period until the crystallization of cyber space, which became aware of it, as an exclusively field, it was defined through internet and network networks and expanded its field with additional concepts and factors day by day [19]. For example, while the concept is defined by experts as a global networked virtual and artificial communication area maintained, accessed and produced by computers in the 1990s [20], in another approach it is defined as a system that hosts the interaction between separate computers and is derived from virtual space (Koepsell). it is stated that the concept is closer to the physical field, referring to the fact that the element that maintains and regulates the interaction between computers is human. In other words, the discussions about the cyberspace medium, which was newly discovered in the 1980s with its unique features, have generally been about both the ontological dimension and spatiality of the concept rather than the content and definition.

The fact that cyber space contains many basic information used and benefited by the people of the virtual-real environment, that is, the existence of the real world and the virtual world, makes a monolithic field discussion about cyberspace meaningless in the new environment of the 21st century. Because cyberspace now has both physical and social structure elements at the same time. It has a physical structure because it finds a place to move by information technology infrastructures, and the reason for its social structure is that the field is started to be considered, spoken and thought by people and institutions. In other words, cyberspace, with its unique tools, contents, symbols and methods, has a certain range of action such as land, air and sea areas. The developments in cyber space-based information technologies and the fact that the human phenomenon, which is the native of the digital world, which is in the background of these information technology tools, naturally takes part in the necessary solution to produce and solve the problems arising from this field, has caused the field to

shape social and political changes. In addition to the increasing number of high-tech tools and information systems day by day, the increasing number of users in cyberspace has both positive and negative aspects in the eyes of the states that are the target against threats from human beings, terrorist groups and a rival state at the same level. As observed in the examples of cyber-based attacks in recent times, cyberspace is the biggest threat area for states in the 21st century due to the threats arising from this area and the late realization of where the risks come from, their indeterminacy and the extent of their content. Because this area provides opportunities that can damage the national security of any state in line with the goals of trans-state criminal organizations and even individuals. And by its very nature, cyberspace offers equal use and benefit to actors at different levels, such as individuals, criminal organizations and the state, but also creates gaps in creating risks and threats. In other words, the risks and threats that may arise from this environment may also originate from individuals, criminal organizations and states, since there are no laws with certain rules and boundaries in cyberspace between the mentioned actors. However, since the identity of the threatening actor in the globalizing nature of cyberspace is no longer attributed, the cyberspace environment creates new and different conditions in the context of security, since in this case the enigma of the threats and risks will create the problem of the perpetrator actor in the eyes of the state.

Increasing awareness of cyber space has brought about the formation of new areas of struggle and policy forms in international relations. In this framework, it has become difficult for states to obtain and maintain power in cyberspace, which has a contradictory structure with its unique features. For this reason, states evaluated cyberspace in the category of low politics in terms of threats and risks to their national security until the beginning of the 21st century, in the category of high politics due to the new threats emerging from the field in the new era and the multidimensionality of these threats. they have developed definitions and measures according to the conditions. According to the definition made jointly by the US Department of Defense, the founder and first user of the Internet through ARPANET, cyberspace is the central system of factors that include the critical infrastructures of their countries such as agriculture, health, emergency call centers, defense industry and technology bases, energy, transportation and communication and banking systems.. Therefore, cyberspace is defined as a system consisting of computers connected to each other, routers connecting multiple networks and fiber optic cables, which allow critical infrastructures to work thanks to these

cables. Thus, the United States considers the continuation of a well-functioning cyberspace area essential for the economic security and, in relation to this, the provision of national security. However, the US Department of Defense, whose awareness of cyberspace has increased after the September 11 attacks, has updated its definitions of the geography of cyberspace, which is changing and transforming with the interaction of communities that use information systems intensively. Storing, manipulating and transmitting data in systems intertwined with computer networks and digitized communication networks, including critical infrastructures, in the national military strategy declarations developed for cyberspace operations by the US Department of Defense in 2006, which he defined by emphasizing the material infrastructures of cyberspace in 2003. described it as the use of the electronic and electromagnetic spectrum with its functionality. However, as mentioned, these definitions, made due to the evolution of cyberspace, which moves at the speed of light, have constantly evolved and presented an anachronistic definition in the perception of US defense in 2009 and 2010. Cyberspace, which is now a platform representing a geography beyond communication and space, which is the manifestation of the intellectual environment in which digitized information is transferred through computer networks, was established by the US Ministry of Defense in 2010 by the networks of information technology infrastructures, telecommunication networks and computer systems. It is characterized as the global area in the information environment that includes integrated processor and control manager [22]. This definition made in 2010 has been handled more comprehensively by emphasizing the impact and dimensions of the field, especially its globality. Of course, this definition expressed by the USA was not compatible with other states. For example, in the UK cyber security strategy, cyberspace is defined as the digital activity that envelops all network networks including the actions and content carried out along digital networks, while Canada defines cyberspace as an electronic space created by interconnected information technology networks. defined. However, since cyberspace has different meanings thanks to the social interaction it has established within the aforementioned networks, with the inclusion of people beyond the internet, which includes hardware, software and information systems, they have started to revise the definitions they have developed in this direction. In this context, in addition to the definition it made in 2011, the UK revised the definition of the concept in 2015 and described it as a digital network area where digital networks that store, change and transmit information, including critical

infrastructure and services, are formed. In the cyber security strategy document of Australia, the concept of internet was preferred instead of the concept of cyberspace, and the definition made was defined as the internet and all the components that make up the internet. NATO, which has established units responsible for cyber defense and implemented activities to improve cooperation and defense capabilities with its members against attacks in this area, stated that cyberspace covers more than the internet. NATO, which is in the process of transforming from a military defense alliance to a global security organization after the Cold War, defined it as a digital world that is manifested by computers and networks of the field, where people and computers can coexist at one point, and includes all aspects of online activities. The UN, on the other hand, defines cyber space, which it sees as a global issue and therefore an area that requires attention with global approaches, as a global system that is connected to the internet, communication infrastructures and means of storing and processing information in the digital environment. In the EU, which has made the issue of information security one of the important strategies of security understanding in the 2010-2020 "Digital Agenda" and has made an effort to produce and develop practical solutions against attacks and threats derived from cyberspace. Described cyberspace as a virtual world where electronic information and inputs of personal computers covering the whole world are navigated. In this direction, the multidimensional and complex nature of attacks, threats and risks arising from cyberspace in the eyes of the states, which are the main variable actors of the international system in the 21st century, have further intensified the debates on the dysfunctionality of traditional threat perceptions and methods of combating these threats, which are claimed to be outdated. Parameters shaped on the axis of globalization in the 21st century have contributed to the security process, as well as to other phenomena of social sciences, in the process of transformation and change in the context of actors, threats, practices and tools. Although these changes and transformations in international relations necessitate new security definitions, people living in completely different conditions and in different places on the globe and other non-state groups can access information via the Internet, lacking geographical integrity and limitations, and without any decision-making control. Considering the dimensions reached by cyber space, which resembles an anarchic system in which there is no mechanism and legal rules, it reveals that states should also put into effect new means of struggle to ensure security. As can be seen, in the changing world dynamics of the post-Cold War era, the increase in the types and quantities of actors and the

emergence of new and mutual relations between these actors, the increase in cross-border activities, the rapid development in science and technology, the change and diversification of the known different and numerous balances [23]. In the 21st century, it has been further strengthened by cyberspace, which has emerged as a new threat and security parameter with its unique basic framework and dynamics. In this case, cyber space, which was almost never considered and aroused interest in the context of its effects on the international system in the international relations community until the 21st century, has now paved the way for it to be discussed in the literary literature on a conceptual and theoretical level. In the light of these issues, Denning has defined the field that he interpreted through information-based processors and information systems as an information environment, and defined it as all kinds of physical structures in which information is used, utilized and stored through printed information, computer and communication systems. Singer and Friedman, who discussed a comprehensive discussion on how the cyberspace works with the basic framework and dynamics of the cyberspace, which brings its positive and negative sides with it along with technological revolutions and paradoxically presents security concerns, risks and threats, also stated that cyberspace is essentially an online use of information. While expressing it as an information environment, the internet of network-based computers, closed intranets, cellular technologies, fiber optics, which combines the systems and infrastructures that allow the flow of this information-based data in addition to the digital data that is created, stored and most importantly shared, in addition to the computers that store this data. He states that it includes cables and space-based communication. Again, it refers to the area that the area is no longer in a homogeneous structure and that formulates information and communication networks, including telephone, satellite and media tools, on the inside, including internet networks. Because, in the 21st century, cyberspace has been multi-layered due to its fast and rapidly growing global nature, and each layer has presented different forms in terms of digital, communication and interaction in communication. In general, Dodge and Kitchin have categorized these layers as internet technologies with processors, cables, software and hardware, and satellites, and conventional telecommunications technologies such as telephone, fax, and media. They stated that the rapid and interconnected development of these categories has revealed a new hybrid field, who stated that considering cyberspace as an internet environment based on its only physical existence, will transform the field into a monolithic structure. Expressing that the sine qua non of cyber space consists of equipment

such as RAMs, processors, motherboards and disks that make up the physical layer, Bıçakçı stated that it would be incomplete to conclude that the physical existence of cyberspace consists only of computer equipment; claimed to have occurred. From this point of view, he stated that the technology that interprets the programming languages of the said layers and the cyber space formed by controlling many components such as the human element will often lead to vulnerabilities at the point of security. Clark, who stated that today it has emerged as a new war environment both on the basis of states and on the basis of sub-state groups, explained cyberspace as a platform for people and communities to be connected to each other as a whole through telecommunication systems that include computers, communication and communication tools without any limitations on physical geography.. On the other hand, Nye and Scowcroft also evaluated the unique tools, qualities and contents of cyberspace, such as sea, air and land space, from an analogical point of view, and especially the fiber optic cables and internet infrastructure that enable the crystallization of the physical layer of cyberspace, as well as international economic institutions and also The importance of the area has drawn attention on the grounds that 65 states' sovereignty falls under their control. Again, by deducing from the similarities, just as the gunpowder revolution in the development of early modern Europe, the Industrial Revolution in the 19th century, a second industrial revolution at the beginning of the 20th century, and the nuclear revolution in the middle of it through technological developments and changes, these centuries left their mark in the political, social and military context. If so, they saw cyberspace, which they see as a turning point in the international system with its speed, tools and unique features, as a platform that left its mark on the 21st century by stating that it is essentially a field of activity related to computers and electromagnetic spectra.

In short, in the light of the definitions made above with its different and periodic dimensions, cyberspace is a platform that consists of interconnected information systems that develop in a time-dependent manner and a series of human users interacting with these information systems, and hosts it in virtual and physical layers with its own decentralized and content. What is meant by the interconnected information systems mentioned here is the transmission medium that connects information, software, hardware and these computer system programs to each other. The concept of human users, which constitutes the key element of the cyberspace field, also emphasizes that it is the human factor that brings this feature to the space that contains artificiality. Because without the user and consumer role playing an

important role in the solution of all kinds of problems in the background of electronic devices and computer system programs, cyberspace will lose its dynamics and eventually cease to be a threat. In addition, another important issue that is not emphasized in the definitions of the concept but is important is the transformation of the nature of the problematic area over time. For this reason, the area, which shows continuous development due to its dynamic structure, is naturally in a position free from statics. In this case, on the other hand, the complexity of the field increases proportionally. At this point, explanations and explanations about the definition of the concept, its content and the effect scale 66 make the emphasis on time variability essential. Although this definition does not constitute a fully appropriate definition for the dynamic global nature of cyberspace, which includes complexity and uncertainties at the spatial, ontological and epistemological planes, a general and concise description has been made by referring to the elements that make up the important parts of the whole field at a minimum level. As can be observed from the definitions made in general, the absence of an agreed definition of cyberspace is striking. In other words, the continuation of the development of information and technology has made it difficult to draw a certain framework for this field and the basic concepts of the field, as it enlarges and expands the dimensions of the final framework of the concepts of cyber threats, attacks, crimes, terrorists, weapons and security arising from the cyber environment.

2.2.2 Cyber Threat

As it is frequently emphasized in the study, while cyber space is a useful area with the opportunities it provides and provides, on the other hand, it has a double-edged sword-like characteristic that contains harmful situations in terms of threats to the national security of states. Although the threats arising from this area, where states remained ignorant until the 21st century, were experienced in previous periods, especially the September 11 attacks, in which information and communication technologies were used first, after the cyber attacks against Estonia, which is a NATO country, increased awareness in the international community and started to take place at the center of the security policies and concerns of the states. and. Considering the widespread use and low cost of information and communication tools, whose homeland is cyberspace, it has become an indispensable field for individuals and most importantly, non-state actors as criminal organizations, and its accessibility, ease of use, and unprovability. and its effect created addiction. The fact that non-state actors

become more and more dependent on information technology tools has led to the emergence of asymmetric new threats in terms of quality and quantity in the international system, contrary to the threat perception of the traditional security understanding. In this context, since these threats of the 21st century are called new, first of all, it is necessary to determine what the old is and in what ways and means the threats called new are different from the old ones. The concept of threat, which is used in the dictionary meaning of intimidation and anger, is defined as the dangers to the core values of the states in the orthodox security understanding of international relations, and the facts that pose/may create risks. While the expression of core values, which is expressed in the definition and explained in the meta-theoretical part of the study, includes the facts of the military and political context in the traditional security perception, this expression also included the facts of the economic, social and environmental context by the Copenhagen School led by Buzan towards the end of the Cold War. On the other hand, in order to define a threat in Williams, there must first be an enemy to which the threat is directed. In other words, Williams stated that the threat needs the other. In fact, Williams, who constructs the ontology of the concept of threat through a defined and concrete enemy or the other, has argued that in this case, any danger directed against the concrete enemy will be a threat. Davis, in the literature of international relations, defined the threat as the intention to cause damage with negative consequences through the possibilities and abilities of a political or social agent.

In addition, Jovi also said that the sine qua non of the concept of threat; It interprets it on the basis of its suitability for purpose, its credibility in terms of capacity and effectiveness and its completeness in the context of its purposes, the fact that the threat is perceived by the party to which it is directed, that it should be harsh and, finally, that it should be clear . Roscini, who described the concept in terms of feasibility in terms of intentions and capacity, also defined threat as a set of dangers that can be clearly identified and measured as a result of the evaluation of the possibilities and capabilities of malicious enemies to reach their goals. For example, a country in the alliance system of the Cold War phase perceived the expansion of military power, vehicles and all kinds of activities and movements in international politics by the enemy state in its opposing bloc as measurable, predictable and intentional threats against itself. David Singer also interpreted the concept of classical security and threat, which he defined and interpreted in relation to it, as the multiplication of capacities and intentions in the context of feasibility. In other words, according to Singer,

the first condition for an event, movement or action to be a threat is its enforceability; In order to be able to perform, it must be persuasive in line with their capacity and their intentions in line with credibility should be visible. As observed, the striking element in the definitions made is that threats are largely based on perceptiveness and probability. Threats can be probabilistic; because sometimes they may or may not happen. However, although there is no clear definition of a threat for all times and places in the historical process, the concept has gained continuity in terms of interpretation in the conceptualization of the concept, which essentially includes the danger of deprivation of the values that states have. In the international system, which manifests itself as a set of interrelated units as a result of the interactions of the states and the way they do politics, the threat element is also military and political phenomena that only pose a danger and risk to the states, in parallel with the orthodox security perception until the end of the Cold War period. Has overflowed from its perceived patterns by the transforming tools of the changing world dynamics of the 21st century. Until now, threats consisted of dangers and risks from one state to another rival state within the framework of traditional security logic. In other words, it was clear from whom, how and by what means the threats came. Therefore, the measures to be taken in the context of defense and attack were shaped accordingly.

The decrease in the size and scale of the conflicts and disagreements among the states, the emergence of different types of actors in different targets, has also presented new types of threats to the international environment of the 21st century and has also taken a place in the understanding of security, which has a direct relationship with the concept of threat. The advanced change and speed of all information tools, including globalization and visibility, communication, internet and computer technologies, which are among the elements that make a new security understanding mandatory, have also transformed the classical semantics and description of the concept of threat. In this context, cyber space, which is composed of information and communication technologies, whose development and spreading phase continues, has left the security of states, which are the main actors of the international system, with a new threat called cyber threats. At least if this conceptualization, in which the basic framework and dynamics are drawn, is followed, cyber threats; With the instrumentalization of the opportunities provided by cyberspace technologies, it falls into the category of dangers that are likely to damage the internal and external orders of social units such as the state, and the political, social and economic core values of social units such

as the post-state. In addition, it has been defined as the danger of causing undesirable situations and results, such as the misuse of information that grows and develops in cyberspace as a purpose and tool, revealing it to the public, or preventing its accessibility with systematic attacks. In this definition, it is emphasized that information tools and systems are used as tools, since cyber threats are only threats derived from information and communication technologies. Wikileaks documents are one of the on-site samples that conform to this definition. As of November 2010, the rapid publication of the records of the USA on the Iraq war and diplomatic electronic correspondence on the Wikileaks website, thanks to the opportunities provided by information and communication technologies, revealed the opinion that cyber space would pose a threat to the states with high technological dependence. So much so that, after the Wikileaks documents, which are called the September 11 of diplomacy by some, Foreign Policy magazine described the cyberspace as the 70th greatest threat to come[26]. Because Wikileaks has not only disclosed the developing technology tools and services and the policies of the states that should be kept confidential, but also shared and reproduced all official correspondence and messages from the embassies and consulates of countries other than the USA in the computer environment. Wikileaks Web site, which was established in 2006 with the tendency to expose corruption and abuse around the world, has posed a threat to the information security of states in relation to cyber space's data and access. As a matter of fact, before the disclosure crisis that has not yet erupted, in 2008, the US Department of Defense stated that Wikileaks and similar websites contained threats against the US army in terms of intelligence, movement and information security. The end of the Cold War not only changed the international system based on bipolarity, but also transformed the nature of the concept of limited threat, which is one of the important factors shaping the way and perception of interstate interaction within the system. Cyber security threats, which nullify the meaning and importance of borders with their decentralized feature, not only accelerated this transformation process but also eroded it [27]. There is no clear and clear definition of the enemy defined in the presence of cyber security threats; The aggressors may be adolescent children between the ages of 12-19, "rogue states" that support terrorism, or terrorists with certain beliefs and ideologies. The decentralization and complexity of cyber threats makes it difficult to verify and authenticate attackers' hostile intentions and threats. A person with computer-based tools can quickly access and take control of someone else's and company's computer in another geography of

the world. Because the advanced state of technology provides this convenience. Attackers, who can access the attack equipment they need along with their experience, opportunities and capacities, can thus carry out cyber attacks by taking advantage of the vulnerabilities of the states in information system security. It was a 21-year-old boy who infiltrated the computers of US federal agencies and accessed information about logistics information systems and used this information to harm different agencies of the government. Again, the person who infiltrated NASA, the institution where the space studies of the USA are carried out, and other institutions of the government's ministry of defense, was 16 years old. has been named. Script kiddies are threats that constitute the lowest class in hacker's ranks. Those who cannot develop their own software generally want to relieve their troubles and curiosity by downloading and using the software and codes they have downloaded from the internet. As observed, widespread vulnerabilities in the information system easily make the desired environment possible for attackers who have knowledge, skills, and even partial experience in this field. In fact, the decentralization of the area, its lack of difficulty and high cost, and the unique possibilities it offers, such as the problem of imputation, have increased the quantity of attackers in parallel with the development of information technologies, and in this case, the number of threats in its natural course has increased. Because the changing characteristics of the information technology environment naturally shape the threat perceptions that will arise from this area, as cyber threats, most of the time, are gaining as a result of the use of malicious and harmful software and hardware with malicious intentions and purposes derived from information infrastructures. In the 21st century, another striking factor in national security and the associated threat perception and policy, originating from cyberspace, is the attacks of individuals or groups that are small in number, and the threats they create as a result. In the classical security understanding, military-based threats that emerged between states could be responded to with an effective intervention. posed significant problems in responding to the When threats are presented to states from sub-state groups, the response of states will apparently be manifested in the context of laws, which brings along some unanswered questions about the clarity, severity and imputation of the threats. For example, is the identity of the attacker or attackers known? Has it been determined who or what is being threatened? And especially because of the advantages that the global nature of cyberspace offers in terms of identity and location, is it clear who is

behind the cyber security threats at the state level? Questions like these reveal cyber threats as a security problem that should be taken into account by the states.

As mentioned above, most of the cyber-based security threats to the states were carried out by individuals or groups called script kiddies, who created a danger by using malicious software and hardware on the internet. Advanced hacktivists, who form the highest level of these groups in terms of knowledge, experience and influence, and who have political, social and religious motives, are another important group that creates a threat with cyber attacks, especially on the critical infrastructures of states that have an important place in the context of national security, using cyberspace. These groups, called hackers in Turkish, aim to inflict serious damage to both the information systems of the states and the critical infrastructures that work dependent on these information systems by using hacking techniques and methods. Examples of these activities are DDOS (Distributed Denial of Service) attacks on government websites, bombed mails, viruses, content corruption and manipulating software and hardware, interruption of internet services, and attack tools such as maggots and bots. In a practical context, cyber-space-based attacks, in which the active participation and realization of the activists, first drew attention in the Kosovo war. Of course, a number of cyber attacks have been carried out in the previous periods. However, with the cyber-attacks of all states and organizations active in conventional wars in the international arena due to ethnic wars, the life of the Kosovo War has been prolonged. The use of information and electronic systems by adopting unconventional ways and using them for attack also creates an unusual threat and a related security perception and practice. In particular, the fact that the critical infrastructure of most of the services provided by the states regarding infrastructure such as almost all financial, military and health, energy and communication infrastructures is connected to information systems, providing a different field of action in posing a threat to hackers who can use the cyber environment well with their knowledge, skills and experience, and style. However, hacking, which creates an unusual type of threat with its application methods, is not a threat method used only by individuals or groups consisting of a small number of technologically skilled individuals. In addition to actors with malicious intentions such as terrorist groups, states can use the cyber environment for attack purposes. Because when cyberspace is evaluated on the basis of reciprocity, it offers almost the same opportunities and opportunities for all actors. Any weak-scale state or trans-state actor wishing to create a security threat from this area need not be strong in the economic

and military context. At the same time, the use of military vehicles in classical warfare periods before the 21st century required professional knowledge, making it difficult for everyone to use; moreover, the high cost of these vehicles brought disadvantages in the eyes of weak states. However, today, if it is organized by a small number of human personnel who have the necessary technological equipment such as a computer and even a mobile phone, and the experience and knowledge of using these equipment, the target of potential attack and threat can be achieved [28].

In addition to the Kosovo war mentioned above, which is claimed to be the first war conducted over the cyber environment, in the tension between Estonia and Russia in 2007, in 2008 Israel used information systems to build the infrastructure of the nuclear facilities that North Korea wanted to build in Syria. Intense cyber-attacks used in the destruction of Pakistan, the Kashmir conflict between Pakistan and India and Israel-Palestine conflicts stand out as examples of cyber-based warfare that can be observed between rival states. it crashes. Cyber attacks against mutual information networks and critical infrastructures fed by these information networks can paralyze the daily political, military and social practices of states and create problems within the framework of national security. These new security threats originating from the cyber environment of the 21st century, where traditional security tools are insufficient to resist, have become even more uncontrollable in the hands of transnational groups that benefit from the blessings of information technologies, and in this context, they have almost led to challenges to the unquestioned sovereignty and authority of states. So much so that the dizzying advances in the field of information and technology have given the opportunity to play important roles in terms of the activities of many different actors from the individual level to the state level, making the functioning and structure of the international system more complex. Until the 21st century, the motto of being the sole dominant actor of the political system bestowed on the state by the Westphalian order was already discussed with the end of the Cold War and, in addition, the globalization phenomenon accelerated by the development nature of information technologies. However, the unique anarchic structure of cyber space, which is the area where all information systems converge at the intersection point, has opened new areas for non-state actors to act in line with their own motives. If, after the Cold War, almost every abstract concept of social sciences has been eroded by containing meanings and dimensions beyond its traditional use in the semantic and conceptual plane, the notion of threat has also begun to erode both on a

contextual and conceptual basis by containing meanings and perceptions that change depending on time and space. In this respect, the factor that accelerates the erosion process of the notion of threat and makes the thoughts reflected in the literature in the form of new threats to be seen frequently is cyber attacks, which remove the meaning of borders and power-based control, and give an asymmetrical threat image with their unique features. The transnational operation of global information networks and the increase in the flexibility of country borders through these networks have invalidated the traditional security approach of the cyber environment, which is the fifth dimension after air, land, sea and space in the 21st century.

The cyber environment has replaced the single, dual or multipolar order observed in the international system with different and multipolarity in which non-state actors can be effective and have a say, and by building an unusual power balance system here, asymmetric power relations that weaken the hierarchy between states, individuals and transnational groups. also brought to the fore. Asymmetric threats, which are described as the aggressor's relatively superiority in spite of his weakness against the addressee, generally aimed to reduce the support of the administrative elements by using the fears of the people of the target country by making use of the vulnerabilities and weaknesses of the interlocutor. Terrorist groups aimed to create political and economic instabilities in their interlocutors in this way, and aimed to make it possible to carry out attacks that cause immeasurable destruction with the help of information technologies that provide easy access. Therefore, due to the sudden and unprepared situation it creates, cyber attacks are comprehensive and trendy forms of action that cause collapses and instability in the political, social and economic systems of countries, aiming to be effective by using low-level technology. Since these new trend threats of the 21st century originating from the cyber environment create an atmosphere in which individuals and transnational groups with malicious purposes can easily access all kinds of information thanks to information technologies, these groups provide an unusual area of influence and movement in carrying out their actions to a large extent and effectively. Cyber security threats, which are unusual with their global nature, have not yet been able to dominate, and therefore do not have certain principles, laws and tools, and which do not have a certain framework about how and at what rate they will respond to threats from whom and how they come from, are still in the Cold War era. The asymmetric threats, which are a new threat quality and type, are also highly visible in the new century. has made. As a

matter of fact, the cyber defense organization of NATO, whose foundations were laid, was accepted in the asymmetric threat category to 76 cyber attacks at the 2006 Riga summit, and then after the 20007 Estonian attacks, it was decided to establish the Joint Cyber Defense Center of Excellence.

In this respect, Özcan pointed out the importance and impact of the area for the states, stating that cyber space, which he sees as the new face of threats and terrorism in the new millennium, will pose the greatest danger to the national security of states in terms of threat types, tools and damages. Because the possibilities offered by cyberspace to trans-state criminal organizations and individual criminals create an unprecedented area of action for these organizations and therefore create public opinion in international challenges against states. For these organizations, whose goals can be political and social, cyberspace easily provides the technology-based attack tools they deem necessary. In this case, developed states that make critical infrastructure sectors dependent on information systems may face threats caused by transnational criminal organizations. Because criminal organizations, which can be at the transnational and individual level, take advantage of the advanced technology offered by cyber space and on top of that, the openness they have, with the opportunities they have of a state's dam gates, all attack and defense systems of military forces, natural gas networks, pressure control, transportation, communication, water, health and banking. They may have the opportunity and ability to seize control of all systems of public institutions, such as state institutions, to lock down and threaten the functioning systems of states. A computer-based technological device with hardware and software will be sufficient for the attackers who will carry out these attacks. Naturally, the tools of cyber threats that derive from the cyber space will be adapted to the cyber environment. For example, the cyber security threats arising from this area create the threat of cyber espionage, while the illegal stealing of valuable and confidential data from rival states through communication networks and hardware and software in order to gain military, political and economic benefit from rival states creates the threat of cyber espionage. It is another new type of cyber threat that makes existing information systems inoperable or manipulates information systems. In addition, damage to the military vehicles of rival states using satellites, especially from information systems, and attacks on infrastructures including oil, natural gas, electricity, banking and transportation services are other important types of cyber security threats.

2.2.3 Cyber Terrorism

As a catalyst for global change, rapid and rapid developments and transformations in the field of information technologies derived from cyber space positively affect the socio-economic and political practices of societies and states, on the other hand, create an asymmetric and multidimensional threat. It has had the opportunity to be an effective tool for terrorist groups that want to achieve their political goals, to create power and public opinion. As Özcan argues, based on the deterministic principle of criminology, which is the branch of science that studies crime and criminal behavior, that crimes follow opportunities, cyber world information technologies make the old threat elements and methods even more complex to malicious terrorist groups and create new threats with new ways and methods. provided opportunities to create an element. Thanks to the opportunities offered by the cyber environment, criminal organizations, as well as the states, benefit greatly from the globalized information and can have fantasies such as explaining bomb-making techniques over the internet; In addition, organized crime groups and terrorist organizations rapidly develop their technical infrastructure with the black money they hold, play the game without being bound by any rules, unlike the security forces, and transfer huge financial resources to this area when necessary, causing states to face serious difficulties in the fight against cybercrimes. In this case, the increase in the diversity of actors to the current complex structure of the international system after the 1990s and the threats caused by these opportunities as well as the opportunities offered to the states by the advances and changes in the technological field have led to an opportunity-threat paradox in international relations. Terrorism in the 21st century is one of the problems that states and the international community have to face with its differentiating aspects, characteristics and complex problems. The conceptual and semantic confusion about terrorism includes reasons beyond just the definition of 78 concepts. The most important problem that stands out among these reasons has been the change in the methods, goals and strategies adopted by the terrorist or terrorists, along with the increase in the tools and opportunities they can access through the possibilities offered by the new dynamics after the Cold War period. The way of doing politics in international relations is changing at a dizzying speed on the plane of actors and actions. In this aspect, the aims of non-state illegal groups, the tools and strategies they adopt to achieve these goals are also changing. Today, all tools in the cyber environment such as all kinds of computer devices, software, internet networks and communication tools can be used easily and easily

by terrorist groups. For example, ISIS found the Cyber Khalifa army (CCA) operating in the internet world insufficient in terms of its capacity to carry out attacks, instead, it endeavored to establish a cyber army in order to increase its intelligence and capacity to carry out full-fledged attacks. By sharing the cyber attack steps in detail, ISIS members opened an online course to expand the cyber soldier network related to their groups, and an ISIS sympathizer started to give lessons on "how to make a cyber attack" targeting western intelligence. As in the case of ISIS, which has recently used the internet effectively as a propaganda tool, these terrorist organizations broadcast in almost every language in order to reach more people and the public on their websites they actively use [29]. States widely use information systems in the military, economy and service sectors. It is striking that states' dependence on information technologies and networks system is not only used by units that are considered legitimacy, but also by terrorists with malicious intentions and other criminal units such as transnational criminal organizations to take advantage of the cyber environment. Terrorist groups, who could not reach the conventional war tools until recently, have had the chance to become a threat to the states and to raise their voices through their actions, with the opportunity to take advantage of the openings and vulnerabilities created by the cyber environment against the states. offered almost equal conditions in the challenges. As mentioned, this increasing dependence of states and societies on information technologies creates different types and types of security vulnerabilities for terrorist groups in achieving their targets of attack on national defense and critical infrastructure systems of states. Today, it is an indisputable fact that terrorism is frequently discussed at both the national and international levels on the conceptual and political plane. However, the threat of terrorism continues to increase steadily in the new dynamics and order of the post-Cold War era. In particular, the actions and challenges of terrorist groups have become more dangerous, fearful and destructive, with the contribution of technological and technical advances in various fields that offer perpetrators opportunities to create threats that are difficult to describe and understand. It is seen that the movement analysis and information processing systems, security programs and policies and strategic methods of private intelligence systems, which are expected to protect people, society and other institutional organs of states, often cannot prevail against these new and destructive threats and adversaries. Strategies and methods developed over the years can sometimes be ineffective in combating this new terrorism with its differentiating aspects and qualities. Because this new terror does

not only use hijacking or suicide bombing as a tool to achieve its goals. Instead, it can use cyber media tools, which are more convenient to use, more accessible and less costly, as a tool. The use of the tools of the cyber environment by everyone, regardless of time, place and rules, has increased the integration of the virtual environment with the physical environment and facilitated the capacity of non-state criminal organizations, which will easily benefit from this atmosphere, to create a new security threat, which they will call cyber terrorism. There are many reasons why terrorist organizations use information systems as a weapon. Cyber terrorism, which creates new threats originating from the cyber 80 environment with its differentiating aspects and characteristics in the new century, is apt to be a subset of terrorism in the classical context. Because cyber terrorism offers criminals options such as concealing their real names or identities, causing possible great harm, influencing the psychological perception of the public of the target country, and being on the agenda in the media. It has also created a smart option for modern terrorists of the 21st century. Considering that terrorist organizations, like states, act with rational logic in carrying out their actions and behaviors and in calculating the consequences of these actions and behaviors, the cost of cyber-terrorism attacks and the possible potentially devastating and disruptive damages in executing their political agenda are very convenient for terrorist groups. creates opportunities. In addition, cyberspace provides terrorist groups with the opportunity to attack more than one target at the same time, thus increasing the impact and severity of the attacks and making it easier to make a sound.

Cyber terrorism or terrorism, due to its different and unique nature, occupies a place on the agenda as the most current and new issue in the national security problematic of states in the 21st century. The national and international system must adapt itself to the threat and possible war environment that cannot be overcome with these new and classical tools. However, before addressing the strategic security policies to be developed and adopted at the national and international level against this different form of terrorism, it is more essential to explain the concept of terrorism, which has not yet been agreed upon, and the concept of cyber terrorism, which has become more complex with the articulation of the prefix cyber to this concept. Before the concept of terrorism is defined and understood, the concept of cyber terrorism will also make it difficult to fully understand. For this reason, the analysis and rhetoric that will be made without understanding the various types and methods that contain the founding elements of terrorism will completely incomplete the abuse and

abuse of the cyber environment by terrorist groups and will further increase the perception of the complexity of cyber terrorism. Therefore, without adapting the founding elements of traditional terrorism such as aims, methods and tools to the concept of cyber terrorism, without identifying the political orientations of classical terrorism and the main elements it contains, without being aware of the terrorist actors of varying quality and quantity all over the world, and in relation to this terrorism. The concept of cyber terrorism will not be fully understood without identifying the divergent goals of the organizations. In the general framework, the real power and effect of terrorism is fear, which is legalized through violence. For this reason, terrorism is an act and it should be defined in this way [30]. Terrorism can be defined as a set of actions that are deliberately carried out by using the fears and concerns of people, groups and societies as a tool in order to resonate with the wider masses. In general, two main motivations direct the daily memorization and practices of human, social and political units; pursuit of happiness and pleasure and avoidance of pain and suffering. Here, the focal point of terrorism aimed to instill fear of terror in the units in question by using violence. In the 21st century, in the 22nd article of the US constitution, which is the country that places the concept of terrorism at the highest level on the national security agenda in the 21st century, especially in the context of the "war on terrorism" developed after the September 11 attacks, terrorism is mostly targeted by sub-state groups or pirate perpetrators. It has been defined as the method of using violence planned or pre-designed with political motivations against non-combatant civilians with the motive of creating repercussions. The sine qua non of the definition of terrorism by the USA is the concept of civilians. In other words, civilians (non combatant) are targeted by terrorists. While terrorist groups target innocent civilians, they do not differentiate between civilians and combatants, as they also target the community. In the United Nations Security Council, on the other hand, political, ideological, racist, ethnic, religious or other concrete and abstract formal concepts can be used to assert its legitimacy by a person or group of people with the intention of creating a permanent atmosphere of terror, for political purposes and attempted in this direction, and defines it as a form of action and behavior that constitutes an element of crime that cannot be considered innocent under any circumstances.

While French law defines terrorism as any activity undertaken individually or collectively with the aim of significantly disrupting the existing public order, through coercion or threat, UK Anti-Terrorism legislation defines terrorism as the use of violence against political

institutions or to leave various segments of society in fear. He preferred the way of defining it as using. Alexandera defined the concept as acts of violence that organized terror groups use and perpetrate against ordinary civilians in order to threaten them with the aim of achieving their political goals or to create an element of fear and horror that can always be felt. However, according to Alexandra, who also evaluated the concept from a historical perspective, she stated that the communication, communication and transportation that came with the rapid technological developments after the 1960s gave terrorist groups the opportunity to easily and easily engage in international and national activities. Just like Wilkinson, according to Alexandra, problems and issues related to terrorism in international relations began to be evaluated in the context of international law only in 1963 and were approved and accepted by international agreements in the early 1970s. In another definition, Jenkins stated that the threat of violence by groups, violent actions of individuals, and violent campaigns aimed primarily at instilling fear can be called terrorism on the other hand, defines terrorism as acts of violence ranging from kidnapping to killing and aiming at intimidation, while in another study called international terrorism, he deals with the concept in a broader and more comprehensive context, that terrorism is more difficult than targeted by the civilian and innocent victims who are attacked or intimidated. defined it as the conscious and planned use of violence or the threat of violence by a group or state without realizing its illegal strategic and political goals by intimidating and intimidating a large audience. In his statistical study on the definition of the concept of terrorism, Schmid stated that there are hundreds of different definitions of the concept and more than fifty percent of them include the words “political” and “fear and terror”. Again, according to Schmid's data, the concept has been defined through violence and the threat of using violence, especially in recent times. The higher the international and intellectual consensus on the definition of terrorism, the higher the conflict over the definition of cyber terrorism. However, definitions of cyber terrorism and the findings put forward ultimately make it easier to define in what ways the characteristics of traditional terrorism, which is a superset, are embodied in the cyber environment. As a result, terrorist groups that can access the new and advanced technological tools of the cyber environment and use these technologies as a tool can carry out their actions such as a political goal and a public mass that is aimed to intimidate. The outstanding game-changing reading on cyber terrorism and its threats, with its new face and dimensions, is a problem of obscurity and lack of information, or worse, too much inaccurate

and manipulated information and information. First of all, cyber terrorism, which is the combination of terrorism in the traditional sense and cyber, gathers under the same roof two important forms of modern fear originating from technology and terrorism, which are notable in this respect. With their differentiating characteristics, these threats can be perceived as more threatening than the recently known threats. In fact, the concept of cyber terrorism has been featured in the international written and visual media, especially from the beginning of the 21st century, and has always been at the top of the ranking and perception of security threats. The global media has tried to scrutinize the issue with eye-catching stories by making analogies with the tragedies in the past, especially the potential catastrophic threats to critical infrastructures. The characterization of cyber terrorism has also been frequently emphasized in the US press since September 11, and almost every case and development from the simple hacking crime to cyber attacks that cause serious financial damage, possible injury and death has been named as cyber terrorism. While this has created some barriers to establishing an understandable and coherent definition of the concept, considerable media attention has undoubtedly played an important role in examining these assumptions and articulating cyberterrorism - with the advantages offered by the numerous security reports. In different studies on cyber terrorism, users of information systems, whether individually or by a group, can pose a serious threat to states and can be one of the essential issues to be dealt with under the title of cyber terrorism. Because, while states argue that their sovereignty is eroded under the threat of cyber terrorism, on the other hand, experts on the subject argued that cyber terrorism should be handled with empirical observations, claiming that the media's only rating-oriented approaches, without relying on any data, exacerbate the problem and therefore detract from objectivity. Again, according to Conway, the concept of national security of the modern era arises as communicative and the central role of the media has an important share in this emergence. Because the political threat perception/image creation environment is used as an effective tool to increase both the openness and availability of information and the concerns and concerns of ordinary people about national security and policy of this information and the method and style of the information environment. From this point of view, the fictional and semantic gap between the assumed dangers and the activities to be considered as cyber terrorism, which is based on a conspiracy-like basis without drawing a theoretical framework, triggers the debates around cyber terrorism; For example, while some present a realistic scenario where the cyber

environment poses a new digital Pearl Harbor threat to the states for terrorists, on the other hand, another group opposes traditional Although they stated that terrorism methods and motivations will be partially observed in cyber terrorism, they argued that analogies such as "digital Pearl Harbor" were exaggerated and that the threats put forward in this scenario would damage the seriousness and theoreticity of the concept. The concept of cyber terrorism was first mentioned by Barry Collin in the 1990s, and although it is not an in-depth definition, the concept has been associated with the use of cyberspace to bring the terms terrorism closer. According to Collin, cyber terrorism has been defined as the abuse of information systems and networks by terrorists with all their components in the international environment. After Collin, the concept was included in the dictionary of security by experts and gradually began to be mentioned in the literature. After Collin's narrow definition, the 1998 report of the Center for Strategic and International Studies, which is one of the first generally accepted definitions, states that violence against information and information systems, computer programs and databases by pre-planned sub-state groups or individuals. It is defined as unlawful threats and damaging attacks against non-combatant units that aim to result in a terrorist attack [30].

First of all, England was the first country to include the concept of cyber terrorism in the terrorism law on the basis of states. According to the UK's terrorism law, cyber terrorism is defined as infiltrating the electronic systems of official units with the motive of influencing the government and society or creating pressure and disrupting the system with attacks. Cyber terrorism, which is defined as attacks carried out using computers and computer systems in the simplest sense, has exceeded the parameters of this definition day by day and has expanded its scope by including the basic elements of the traditional concept of terrorism. In another definition made in the mid-2000s, fard-i mahal is defined as the use of information systems to intimidate, intimidate or pressure state institutions in order to reach the goal of creating a political, psychological, socio-economic, prestige, and most importantly security threat by an organization. It has been defined as being used to keep it under. In the definition of the FBI, which is responsible for the domestic intelligence and security of the USA, cyber terrorism is defined by computer users within the scope of communication and information facilities to disrupt or stop the functioning of critical infrastructure systems that provide public services in order to adapt governments or society to certain political, social and ideological agendas. It has been described as criminal acts that

tend to create a fear with the intention of and, as a result, cause confusion in society. In Colarik, he stated that cyber terrorism should include attacks against the global information infrastructure, and stated that terrorists attack these information infrastructures and they plan to perpetuate not only the climate of fear but also violence. In line with the understanding accepted as a type of traditional terrorism mentality, cyber terrorism is a type of terrorism that politically motivated groups use to carry out their destructive and malicious actions through computers, information, advanced networks and technological infrastructures. Considering these critically important elements managed by information systems and the internet, many experts argue that cyber terrorism may become more dangerous than terrorism in the traditional context in the 21st century. In this context, the reality is that the targets and risks associated with cyber terrorism acts are posed to governments' valuable records, air traffic controls, dam controls, medical records, and financial and commercial infrastructures. In the light of the above definitions, the observed reading of cyber terrorism includes the political and social motivations of the actions and the fact that they are presented as computers, networks and information systems, and targeted motives such as injury, serious damage, climate of fear and death as the aim. Emphasis is placed on the necessity of being Maras also drew attention to cyber terrorism by stating that cyber terrorists aim to attack critical infrastructures in order to intimidate states or force them in line with their aims due to political, religious and ideological reasons. For this reason, he stated that this new threat of the 21st century may target the critical infrastructures of the USA in order to harm its economic elements and that it may even cause loss of life87. On the other hand, according to Maras, every action or attack by individuals or organized terrorist groups originating from the cyber environment may not constitute cyber terrorism. Along with Conway, Maras stated that the first points that come to mind in the common definitions of cyber terrorism should cause destruction and even death, and that it should be put into action with political and social motives. In this case, according to the statements of Maras and Conway, cyber terrorism can be included in the category of terrorism if it is a development that causes large-scale destruction or death on its own. As mentioned before, cyberspace is poised to become an important battleground that has started to become popular for various non-state actors to carry out their political attacks and actions and to make their voices heard for propaganda purposes. In particular, according to the 2009 report published by the Estonia-based NATO organization, the increasing influence of non-state actors in international relations and the

cyber attacks and network infiltrations originating from the cyber environment that they carry out by hiding their identities play an important role in setting the agenda. The 2007 Estonian attack and the 2008 Georgian attack can be just a few examples. Until recently, the most popular cyber attack, which was carried out with political motives and known to everyone, was the attack in Estonia in 2007. In this attack, the DDOS 89 attack method, which was used to prevent the target user group from using computers and computer systems, was used and the websites of Estonian government institutions, banks, media organizations and private companies became inoperable and many functions in the country became inoperable. Although the cyber attacks that lasted for about a month after the removal of the Red Army monument they established in Estonia, which they liberated the Russians during the Nazi occupation, could not be proven, it was thought that the Russian intelligence and its attackers carried out this action with political motives due to some findings in NATO. However, another important parameter of cyber terrorism that is compatible with the theoretical concept of traditional terrorism is the element of fear. In this context, when the fear factor is considered around the concept of cyber terrorism, just like in traditional terrorism, it can be defined as effect-oriented and intent-oriented. Accordingly, in the effect-oriented definition, cyber terrorism is defined as an atmosphere of fear created as a result of attacks carried out through any of the information systems and having a sufficiently destructive effect, while in the intent-oriented definition, cyber terrorism is to intimidate states and their societies with illegal and political motives or to intimidate these units. It is defined as illegal actions carried out through information systems to force acceptance in achieving their own political, ideological and social goals. Perhaps, these two definitions can be observed as a simplified definition within the framework of traditional terrorism, as it only focuses on the climate of fear. However, the fear factor, which is one of the important components of cyber terrorism, should be considered from two perspectives. The first is that fear and confusion have always arisen as a result of the inconsistent features of cyber terrorism in terms of level and dimensions, due to the mere nature of cyber terrorism. Because the striking feature of the threats emanating from cyber terrorism is obscurity, lack of information or fear of being misinformed. In this case, the notion of cyber terrorism has brought with it two important fears that have emerged from technology and terrorism in the recent period, since it includes both technology and the terrorist threats originating from these technologies [31]. Secondly, the increasing dependence of states and

societies on technology can lead to significant chaos and loss of control over their survival and management in case of large-scale cyber attacks. In any case, creating fear, chaos and confusion is the main purpose of cyber terrorism. In short, there are many reasons why cyber terrorism, whose conceptual and qualitative features are drawn above, is interested in units that have malicious intentions both compared to traditional terrorism and with the opportunities it offers. First of all, the cyber environment is less costly in terms of financial and human resources, methods can be applied more easily without the need for the use of advanced technological tools (sometimes a mobile phone, sometimes a tablet, laptop, etc.), the perpetrators cannot be imputed to their identities, at the same time. Factors such as the ability to target multiple targets in a short time, the novelty of the attack, and thus the attractiveness of the attack, provide the opportunity for more comfortable and effective propaganda in the press and visual media, providing the environment they need to achieve their goals [32].

2.2.4 Cyber Warfare

In doctrinal arguments, war is not defined as a very different and autonomous phenomenon from political processes, but as a means of overcoming the issues and maintaining the policies of states with other methods [33]. In this respect, Tilly refers to the importance of war in the establishment of states by saying "states make war because wars establish states" [34]. The concept of war, along with the motto of the state, which emerged as the only political model after the Westphalian order, has also been defined within the framework of international law [35], which is defined as the set of rules regulating the relations and behavior patterns among states. According to this, war is an armed struggle that more than one state wants to impose against each other, or with political and economic motives, within the framework of the rules regulated by the law of the states. At this point, the only argument that can be put forward regarding the unchanging essence of the phenomenon of war is that the concept will continue to exist as a political instrument in the future as well as in the past to protect security when appropriate [36]. Because in the anarchic environment, the possibility of war with each other is always possible. However, due to reasons such as technological developments, non-state actors whose visibility and effectiveness is increasing in the international security environment, and globalization, the phenomenon of war, which is traditionally seen as the most brutal political tool under the monopoly of nation-states, has

been questioned [37]. At the conceptual level, the phenomenon of war has embodied a type of knowledge required by the specific conditions and context of each period in the historical process. In this context, the phenomenon of war, classically perceived as a primary security threat, now includes new warfare tools and attributes originating from cyberspace and new threats to security [39]. For this reason, possible war situations against the national security threats of the states observed in the past now include new types of wars that pose a threat with different goals, strategic goals and tools on the security agenda [40]. The new type of war of the 21st century makes the ambiguity between the state of war and the state of peace more evident than the old one, but also makes it different in terms of quality with elements such as asymmetric warfare, terrorism and irregular warfare. Cyber warfare is one of the types of war in which both states and sub-state groups can weaken the status quo powers through asymmetric warfare against states, regardless of strong or weak discrimination. Technologies originating from cyber space, which has emerged as a new field of action after sea, air, space and land, as a result of the developments in technology and the increase in the use of computer systems by some, have created new security threats and the actions as a result of the reactions to these threats have revealed the phenomenon of cyber warfare in the 21st century. While this new type of warfare does not abolish classical warfare, it has the potential to transform its form and quality. Because when compared in terms of the methods and methods of traditional warfare, cyber warfare; It is difficult and sometimes impossible to detect where the attack is coming from, 92 Light speed, mostly effective in the field of information and communication systems, the combatants can be a person, a group, an organization or a state, it is usually cheap in cost. It is possible to be effective with a computer, chips are computers or other hardware used in information systems, software is the biggest weapon, often very high technical and technology is not needed, the attack may not be noticed in terms of signs of attack, and finally it is very difficult to determine where and how much damage has occurred. In the light of these issues, cyber warfare, one of the fourth generation warfare types of the 21st century, has changed the form of classical wars. This type of war, which removes the concept of the front from being a spatial phenomenon anymore, has become one of the most important war fronts in the cyber world, and especially in times of peace, crisis and war, it can be performed multidimensionally, with sabotages that destroy the information infrastructures, to discredit the enemy power, to weaken the morale, and to destroy the morale. Cyber attacks carried out to gather intelligence through

secret infiltrations have become one of the important parameters of the new generation war [41]. This type of war, which adds different dimensions to the transformation in the content of the traditional war concept in terms of method, purpose and means, is also expressed as asymmetrically. Because technological innovations, which tend to adapt to weak units in terms of war strategies and the needs of states, provide an enemy state with high technology the opportunity to create a security threat with technological methods in a remarkable way. Because you do not need to be strong and financially rich in order to perform the war techniques that will be needed in wars originating from cyberspace. This naturally leads weak states and terrorist groups to adopt cyber warfare, perhaps faster than technologically strong and advanced states. Today, it has become popular to use information systems as a tool and purpose both between states and in asymmetric wars of different units with states. Because the unique anarchic nature of cyberspace gives the opportunity to open asymmetric fronts for trans-state groups in case of an asymmetrical war. It is true that the impact and destruction of a well-organized and planned cyber-attack can be at least as devastating and deadly as that of a classical war. And even according it is a fact that there are discussions about whether operational cyber wars should replace traditional military operations in order to be more effective in military operations. According to Derian, in addition to the new technologies of imitation and simulation, tracking and tracking capabilities and speed; The shortening of the area, geographical distances and chronological time between real and virtual warfare has led to the development of the concept of war by carrying meanings beyond the known meaning. Of course, as mentioned above, threats and wars have become asymmetrical through cyberspace, transforming the contents of concepts in direct proportion to transforming security asymmetrically. However, according to Carr, who defines cyber warfare by referring to Sun Tzu's strategy of winning war or battles without fighting, which makes a credible contribution to the historical and conceptual evolution of the classical concept of war, this new type of war is the art and science of defeating the enemy without fighting and shedding blood. described as. In addition, the use of cyber warfare methods to prevent, eliminate and use/exploit the function of all military and civilian information systems and infrastructure of another country by a country or on its initiative in order to fulfill the national goal of cyber warfare or to support an ongoing war, and with this related to it, it is defined as measures or processes to be taken against it. In Özdemir's definition, cyber warfare can also be used as a tool to support traditional wars. The United Nations

Glossary of Terms has also defined the concept as a type of war waged by computer systems to cause damage to or destroy enemy systems (Department of Defense Dictionary of Military and Associated Terms (Joint Publications 1-02). The common feature of these definitions is cyber warfare. In this case, it becomes normal for states to attack each other by targeting each other's information networks and systems. In addition to creating significant advantages in the military wing, these technological developments and tools also create disadvantages for the same military wing, because countries' informatics, whether directly or indirectly - especially critical infrastructures and industrial centers- It should be considered that the rational method to be used by the parties during a war would be to obtain the target country's information systems through smart software and to prevent or collapse them. Of course, this new type of warfare, which does not abolish the traditional war type in practice, has sometimes been used as a tool in classical wars with its indirect contributions, and sometimes it has contributed to transforming the form of classical warfare in the 21st century by being carried out as a purely cyber warfare in a different battlefield free from classical wars. Mostly, cyber warfare includes six actions in the form of psychological and electronic warfare deception, physical destruction, information attack and security measures [41]. In terms of targets, political targets, which include the public centers of states, ministries, strategic command centers and units supporting these centers; It consists of structural targets including fiber optic networks, computing centers, network and satellite links, financial centers, air and ground traffic control centers and energy centers, and finally military targets including warning sensors, defense and control command centers and electronic weapons systems. According to Richard Clarke, who was appointed to the presidency of the USA as a cyber security expert in 2001 and made a generally accepted definition on this subject, cyber warfare was defined as the infiltration and penetration activities of a state with the aim of damaging or disrupting another state's computer systems or networks [42]. In this definition, which sees cyber warfare as the field of activity of states, the basic criterion is to damage the systems of the counter-state and to carry out preventive attacks against the functionality of the systems. For example, the attacks by Israel of the nuclear facility that the North Koreans tried to build in eastern Syria in 2007, to deceive and manipulate Syria's air defense systems connected to information systems, exemplifies this definition (Clarke and Knake, 2010). Again, as a result of the uninterrupted – although not certain – attacks of pro-Russian patriots against Estonia, one of the countries that rely on the internet the most, the

collapse of Estonian state public institutions and organizations, banking services, communication and trade services for about a week is another matter. constitutes an example of cyber warfare. Unlike cyber warfare , which is a continual an on-going threat, the concept of cyber war is a topic of debate. Part of the problem of defining cyber war comes from a mish-mash of other terms such ascyber terrorism, hacking, cyber espionage, cyber crime, cyber identity theft, phishing and so forth.When does a hacker become a cracker—some-one who electronically breaks into a supposedly

3. MATERIAL AND METHODS

3.1 MACHINE LEARNING (ML)

The method of enabling computers to learn what to do through algorithms instead of giving the necessary steps to solve every problem in advance is called machine learning. Machine learning algorithms are dynamic structures that create models using a large number of content and can find solutions by predicting the problems that may be encountered later [43]. These algorithms recognize patterns and train on decision making using large data input and output sets. With enough repetition and modification of the algorithms, the results and estimates of the inputs are compared, and the predictions of the next results are close to perfection [44]. Inputs such as text files, tables, databases are displayed in a structured format through the selected algorithm and machine learning is realized by generalization [45]. Various measures such as accuracy and precision are developed to define the quality of the algorithm, and accurate information is provided with statistical methods such as confidence intervals and standard deviation [46]. As can be seen in Figure 3.1, the data in the training set is modeled by training through the defined algorithm. Then, a machine learning algorithm is developed over this model, and the data in the input set can be processed with this algorithm, and model estimation can be made.

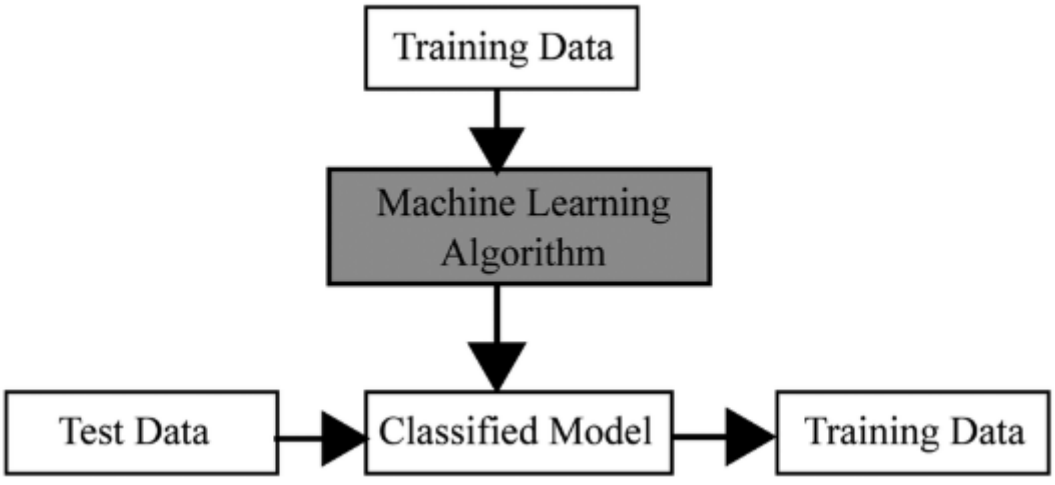

Figure 3.1: General process of Machine learning

In short, machine learning is the process of obtaining information outputs from the data entered with calculation methods [47]. machine learning; In addition to learning complex patterns through modeling, which makes predictions about data, it also has the ability to interpret what has been learned [48]. Being able to perceive input data by associating it with

its outputs [49]; One of the prominent features of machine learning is that it can change the thinking system based on experience. Computer systems showing the performance of a human in a task; It is possible with machine learning to analyze independently from their task areas, simulate the cognitive process and learn from experiences. Machine learning, which is defined as the improvement of behaviors over time with the development of learning paradigms, is based on two different paradigms as Supervised Learning and Unsupervised Learning. In supervised learning, the inputs and outputs, which are the training data, are labeled and the machine learns with these labels. The supervised algorithms provide the accuracy of the predictions during the training with feedback. Predefined inputs and known outputs are labeled and trained, and the model is used to represent the learned relationship between input and output parameters. Supervised learning algorithms; Examples are K-Nearest Neighborhood (K-Nearest Neighbor), Decision Tree (Decision trees), Bayesian Statistics (Bayes statistics), Support Vector Machines and Neural Networks (Neural networks). K-nearest neighbor method; It is the classification of the data sample based on the labels of the nearby data samples. decision tree; It is a classification method for estimating data labels by repeating entered data. neural networks; They are algorithms used to recognize nonlinear and complex functions. Support vector machines; It is a machine learning algorithm that learns to classify data points using labeled training examples. Bayesian statistics; Unlike most machine learning algorithms, they are algorithms that work with a relatively small number of training examples. In supervised learning; mostly, instructions on what to learn and how to learn are given clearly from the beginning (Çolakoğlu, 2020). On the other hand, in unsupervised learning, the tool learns by making inferences from the inputs without any explicit feedback. There is no output vector and no labels are given to the inputs. It is aimed to classify them into different groups by investigating the similarity between the sample sets. K-Means Clustering and Principal Component Analysis are examples of unsupervised learning algorithms. K-means clustering; Used to describe different sets of data. Principal component analysis; It is a multivariate method that aims to extract important information from data and is used to reduce data compression and dimensionality by introducing a number of new variables (Alsheikh et al., 2014). In unsupervised learning; The inputs of the parameters are evaluated within themselves and the target is not specified [50]. Introduced as a technique for artificial intelligence in the late 1950s, machine learning has recently been used for applications such

as speech recognition and computer vision for a wide variety of tasks including classification, regression and density estimation [51]. At the same time, machine learning methods can be applied flexibly to changing inputs and the flexibility of business processes can be increased, constantly improving performance (Koehler, 2018). In machine learning, the need for models to be transparent and to be checked frequently can be seen as disadvantages [52].

3.1.1 Artificial Neural Networks

Artificial Neural Networks (ANN), that is, artificial neural networks, which are mathematically modeled by being inspired by the nerve cells that provide learning in the human brain and enable the computer system to perform machine learning with a similar approach [53]. They are computer programs that learn classified information using neural sensors and can make decisions by producing new information. Artificial neural networks (ANNs) have learning and memory functions with the ability to reveal the relationship between data. In artificial neural networks that learn with the help of examples, each nerve has a weight value and its knowledge is spread to the network. The purpose of these electronic models, which are based on the neural structure of the brain, is not to create a copy of the human brain, but to be able to produce human-specific solutions and make calculations in order to make inferences. By learning from their experiences, artificial neural networks can reduce the information they have learned to general and draw new conclusions. He can even catch the essential essence by removing the parts of the newly acquired knowledge that he deems unnecessary. In artificial neural networks; Neurons in the human brain are called units. In these networks consisting of many units, each unit is connected to other units and signal exchange takes place with this connection. The units, which are connected to each other with certain weights, obtain the information from the outside with the collection function, produce the output through the activation function and transmit it to other units with connections. In layers parallel to each other; The information entering from the input layer is processed in the intermediate layer and reaches the output layer. In order to reach the correct output, the correct weight value must be given to the inputs. Learning rules reinforced with each example shown to the network ensure that the network is trained. Difficulty in combining the information that is distributed to the whole network with weights

and which needs explanation about what it means later is seen as a disadvantage of artificial neural networks and causes it to be called a black box [55]. The adventure of artificial neural networks, which started in 1943 with the article written by McCulloch and Pitts on neurons working with a simple neural network model they created with electrical circuits, has risen with the emergence of Perceptron, the oldest neural network [56]. Inspired by biological neural networks, artificial neural networks are massively parallel computing systems consisting of simple processors with a large number of interconnections [57]. Artificial neural networks, which can solve nonlinear multivariate problems without being affected by noisy data sets without the need for detailed information about the problem or process, can provide solutions with the same modeling even for problems of different qualities, with their parallel structure and easy use on hardware [58]. Artificial neural networks are used by business administrations as a decision-making and forecasting tool in terms of making more accurate predictions compared to other forecasting models [60]. Artificial neural networks used in prediction, classification, correlating and interpreting data or filtering; It has flexibility and error tolerance to work with missing data [61]. The fact that each of the artificial neural networks used in many problems that are difficult to solve offers different solutions, is of great importance in solving the problem that needs to be used. Backpropagation network (Back propagation network), Multi-layer perceptron (Multi-layer perceptron) and Radial basis function (Radial-based function) are some types of artificial neural networks [62]. The fact that they need excessively long training and learning time in solving real life problems, their characteristics constantly change during the learning phase, they can learn from long repetitions [63], there is insufficient information about which structure should be used for which problem [64]. This causes artificial neural networks to be weak in terms of reflection.

3.2 EXPERT SYSTEMS

Systems that can act as an expert in the relevant field in the face of a limited problem and integrate the features of having comprehensive knowledge and performing tasks into computer programs in order to produce solutions through artificial intelligence algorithms are called Expert Systems, that is, expert systems [65]. Expert systems that offer results close to human reasoning can be used as decision elements, as well as as decision support elements in complex problems and offer suggestions [66]. 15 The program, developed by Edward

Feigenbaum, is characterized as the first expert system as it imitates a process similar to decision mechanisms [67]. Expert capabilities embedded in the software algorithm are used by expert systems to create new judgments and recommendations [68]. Expert systems bring solutions to problems in a way similar to the human decision-making process by using the expert knowledge and experience previously transferred to the knowledge base [69]. Expert systems used by non-experts; While it is supportive, it reinforces decisions when used by experts [70]. Expert systems that try to emulate human decision-making ability and solve complex problems by using the knowledge base are a kind of reasoning systems. Expert systems, which follow a hierarchical approach in problem solving, combine low-level information from different points and increase existing expertise. The knowledge base, which consists of a database and rules, the user interface, which is the communication tool from which the information about the actual situation is received, and the inference mechanism in which the information is processed constitute the basic components of expert systems. All expertise information stored in the knowledge base is filtered by the extraction mechanism, interpreted and results are obtained. The result is delivered to the user via the user interface [71,72].

As the complexity of the system increases, the demanded computing resource increases and this slows the system down. In order to prevent this, the cost of expert systems that need to be developed and maintained is high. Expert systems; The requirement to precisely match the input data with the rules makes the reasoning sensitive. This system, which replaces the experts, aims to solve the problems accurately and quickly, increasing the working efficiency and the quality of the decisions taken. Expert systems; While being based on a logical cause-effect relationship, providing reliable information and suggestions, and being able to work with uncertain data and rules, express their strengths, the difficulty of obtaining information, the inability to renew themselves by learning, and the high cost of development can be counted as their weaknesses [73,74].

3.3 DEEP LEARNING

Deep Learning, which is a part of machine learning, consists of data representations connected with deep neural networks. It carries information from low-level parameters to high-level parameters through different layers. These different levels correspond to different levels of data abstraction that lead to learning [75,76]. Deep learning computes the

representation of a machine in each layer from the representation in the previous layer. It uses the back propagation algorithm to determine how it should change the parameters used for this calculation and explores the complex structure in large data sets [77,78]. Deep learning, which is the version of artificial neural networks that works with more units and layers, covers computational models with more than one processing layer. It represents the data with different layers on top of each other [79,80], it learns from raw data and integrates large datasets to reach feature sets. Representation learning is a set of methods that allow a machine to detect by feeding it raw data or automatically discover the representations needed for classification. Deep learning is a representation-learning method with multiple levels of representation, obtained by creating simple and non-linear modules that transform each representation from raw input to representation at a higher and more abstract level [81]. Deep learning, which can carry out many processes together, automatically performs feature extraction in which the features of the desired structure are determined in the network with the preprocessing and hierarchical structure between the layers [82]. Deep learning, popularized by Hopfield and Rumelhart, enables previously stored or used information to be used in new experiences [83]. Since deep learning models learn directly from data, a large amount of data is not needed to train [84]. Deep learning, which includes but is not limited to speech and vision functions through neural networks, which are very good at discovering complex structures in high-dimensional data [85], Natural Language Process (natural language processing), Speech (speech), Vision (computer vision), It is used for different purposes in various application areas such as information access and multiple learning [86].

3.4 GENETIC ALGORITHMS

Inspired by the natural evolutionary process, Genetic Algorithms, which works with selection and crossover methods in a complex multidimensional search space, is a population-based heuristic optimization method that creates new points in the search space [87], based on the survival of the best. It is a method of searching for the best solution. Finding the one that gives the best results from different possible solutions to a problem is called optimization [88]. Genetic algorithms, which are different from traditional optimization methods, work with the coding of variables and can process several designs at the same time by improving them in a way that they can be applied to the search field with random operators. For the solution, clusters consisting of many structures are formed instead

of a single structure, and clusters representing many possible solutions are described as populations. Genetic algorithms, which emerged in the 1970s, are a search and optimization technique that transfers Darwin's theory of evolution to the computer environment by simulating the principle of natural evolution, that is, the survival of more adaptive living things and their genes [89]. It enables to choose the most successful hypotheses and find the rules that best explain the data. Genetic algorithms, an artificial intelligence-based search method, were first developed by John Holland. Being able to search for probabilistic characters and multiple possible solutions are two of the most important features of genetic algorithms. Genetic algorithms, which search effectively by scanning not the entire solution space, but a certain part of it, can reach the global one without being stuck with the local best solutions by reaching the solution in a short time and examining the population consisting of the solutions at the same time. In genetic algorithms, each solution corresponds to a chromosome, while each parameter represents a gene. Genetic algorithms that use crossover and mutation, which are natural selection functions, to solve the problem, make a selection by evaluating the fitness functions chosen for the suitability of each solution. This choice; The initial population created in the range of 0-1 consists of a subset of all solutions randomly, and the randomly generated individuals, each of which is co-coded to a chromosome, are evaluated according to the fitness function by rounding to 0 or 1, and after this evaluation, it is determined whether they are good by passing through the objective function. The suitability of the determined solutions is measured in the fitness function, and separate fitness functions are determined for each problem. By preserving the best solutions in each generation and transferring them to the next generation, genetic algorithms become reliable with the selection method that makes the whole population better from generation to generation. During the gene swapping made by crossing during the mating process, an element of the chromosome is changed with the mutation method, thereby changing the direction of the search and facilitating the search. In the mutation process, the diversity of individuals in the population is preserved and the genes in the chromosomes are changed randomly and progress towards the global optimum. After the selection function, two new solutions that have never been tried before are produced with the crossover function, and this process, which ends with the mutation function, is constantly repeated until a new population. In the selection function; There are three functions: the planted selection, which gives the best solution a chance to live, the random selection that randomly chooses from

the obtained solutions, and the elite selection that constantly transfers the best solution from generation to generation [90].

3.5 PROPOSED METHOD

In this study, hybrid deep learning framework presented for SQL injection as cybersecurity application. The proposed method consist from several stages as shown in the below protocols:

a) Start python code.

b) Read the SQL dataset

c) Applied CNN to extract high level features from input SQL inquiries to decide if these codes are normal or abnormal.

d) Random forest applied to classify the features of the SQL and try to learn the features to decide these features labels are normal or attacks.

e) The genetic algorithm applied to enhance the performance of the model by updating the weight and basis and present best accuracy rate.

f) The selected best model used to predicate the results.

g) Complete

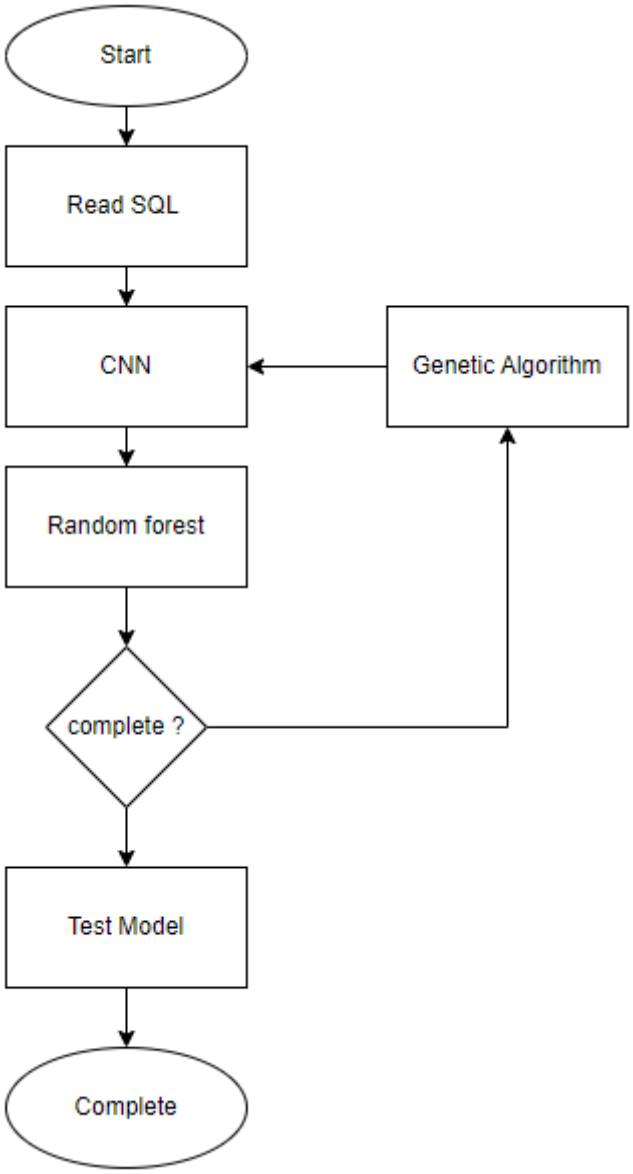

Figure 3.2: Proposed method

4. SIMULATION RESULTS

In this section the simulation of this system validated using several validation techniques with several techniques. The validation techniques aim is to void the overfitting problem. Then, several techniques applied to recognize human hand images.

4.1 CROSS VALIDATION

This is the humblest assessment technique and is extensively castoff in Machine Learning schemes. Now the whole dataset(populace) is split into 2 sets – train set and test set. The data can be split into 70-30 or 60-40, 75-25 or 80-20, or even 50-50 dependent on the help issue. As a ruling, the amount of training data has to be larger than the test data.

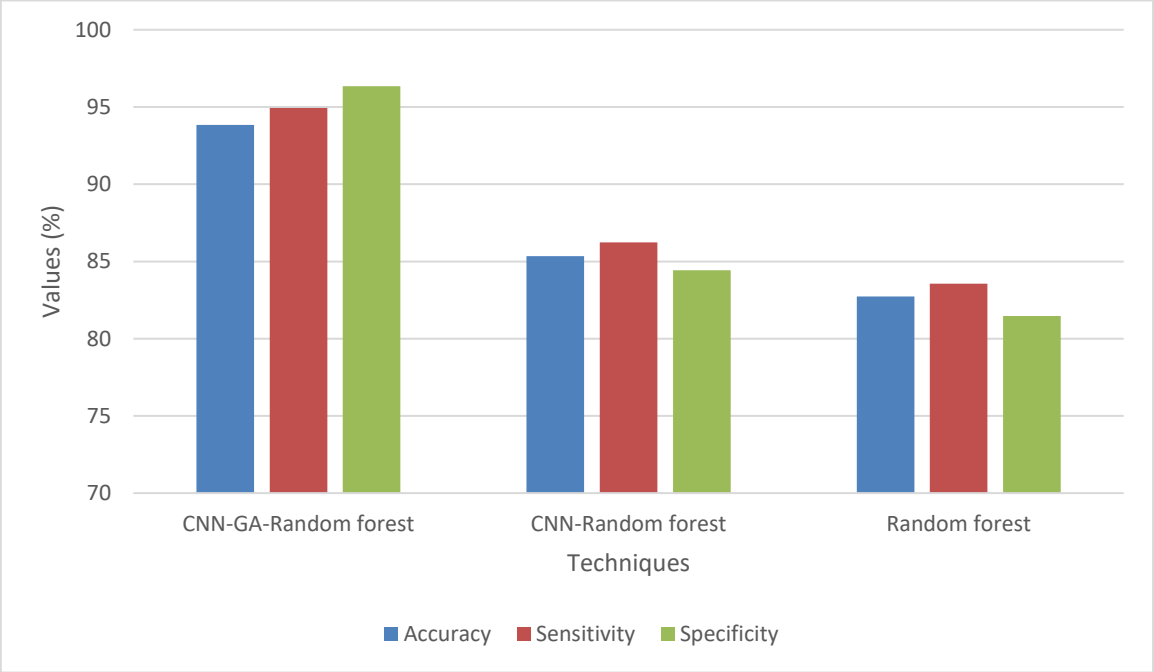

Figure 4.1: Cross Validation

4.2 HOLD OUT METHOD

In this process, we divide up the data into train and test sets – but with a twist. Instead of splitting the data into 2 subsets, we choose one observation as test data and mark the rest as training data and the model is trained. Now the second observation is selected as test data and the model is trained with the remaining data.

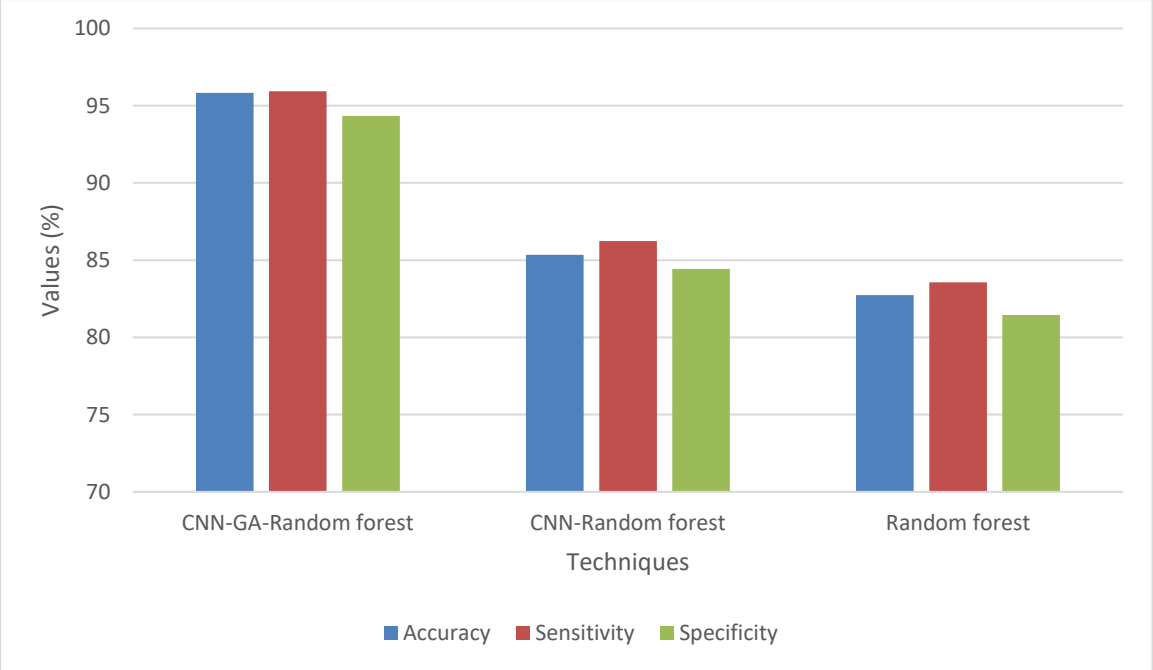

Figure 4.2: Hold Out method

4.3 LEAVE ONE OUT CROSS-VALIDATION

In this process, we divide up the statistics into train and test sets – but with a pull. In its place of separating the data into 2 subgroups, we choose a separate study as test data, and all else is categorized as training data and the simulation is trained. Today the 2nd study is chosen as test data and the model is trained on the continuing data.

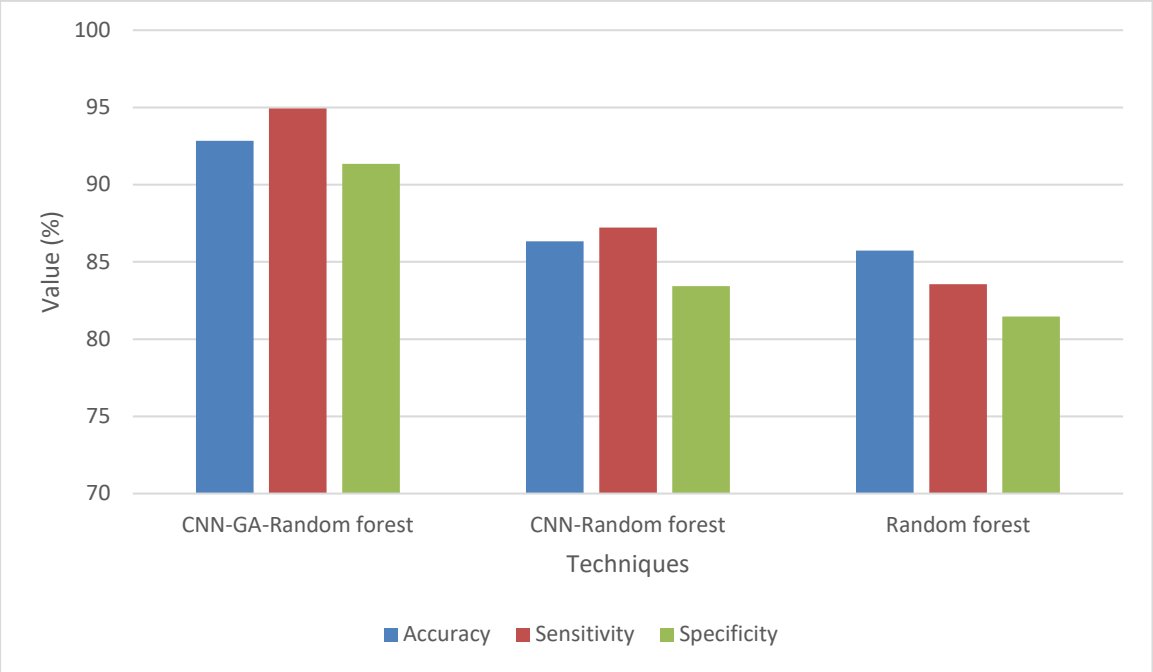

Figure 4.3: Leave One Out Cross-Validation

5. CONCLUSIONS

SQL injection is the most common cyber security threat in all systems with database infrastructure. If you have such an infrastructure, you should definitely take the necessary precautions. In this study, we propose new study based CNN-GA-random forest to detect the SQL injection attacks in IoTs. In the first stage, the CNN applied to extract high level features from input SQL inquiries. Then, the output of the CNN wired to the random forest. The random forest is robust classifier used in several classification and regression problems and presented remarkable results when compared with other classifiers. Then, the genetic algorithm applied to train the CNN to select best weight and basis of the model. The genetic algorithm is robust optimization algorithm and used in several fields to enhance the performance of the models such as design, classification, regression and estimation. The proposed system showed results with an accuracy of 99.93% compared to some studies. Furthermore, several validation techniques applied to prove the performance of the proposed method.

In the future works we advises researcher to applied new structure of convolutional neural network to detect SQL injection attacks in cybersecurity applications. Furthermore, we applied other algorithms instead of genetic algorithm to enhance the performance of the CNN.

REFERENCES

[1] V. P. Nigam and D. Graupe, “A neural-network-based detection of epilepsy,” Neurol. Res., vol. 26, no. 1, pp. 55–60, 2004.

[2] A. Abraham, U. States, and C. Grosan, “Genetic Systems Programming,” vol. 13, no. May, 2006.

[3] L. Deng and D. Yu, “Deep Learning: Methods and Applications,” Found. Trends® Signal Process., vol. 7, no. 3–4, pp. 197–387, 2014.

[4] K. Ahmed, K. Nia, S. A. Khan, and A. Shaukat, “Identifying Be est Feature Subset for Ca ardiac Arrhy ythmia Classification,” pp. 494–499, 2015.

[4] A. Shenfield, D. Day, and A. Ayesh, “Intelligent intrusion detection systems using artificial neural networks,” ICT Express, vol. 4, no. 2, pp. 95–99, 2018.

[5] A. Kaushik, H. Gupta, and D. S. Latwal, “Impact of Feature Selection and Engineering in the Classification of Handwritten Text,” 2016 Int. Conf. Comput. Sustain. Glob. Dev., pp. 2598–2601, 2016.

[6] A. Gupta, A. T. Müller, B. J. H. Huisman, J. A. Fuchs, P. Schneider, and G. Schneider, “Generative Recurrent Networks for De Novo Drug Design,” Mol. Inform., vol. 37, no. 1, 2018.

[7] S. Ibrahim, R. Djemal, and A. Alsuwailem, “Electroencephalography (EEG) signal processing for epilepsy and autism spectrum disorder diagnosis,” Biocybern. Biomed. Eng., vol. 38, no. 1, pp. 16–26, 2018.

[8] N. Kohli, N. K. Verma, and A. Roy, “SVM based methods for arrhythmia classification in ECG,” 2010 Int. Conf. Comput. Commun. Technol. ICCCT-2010, pp. 486–490, 2010.

[9] V. Sze, Y.-H. Chen, T.-J. Yang, and J. Emer, “Efficient Processing of Deep Neural Networks: A Tutorial and Survey,” vol. 105, no. 12, pp. 2295–2329, 2017.

[10] D. Petkovic et al., “SETAP: Software engineering teamwork assessment and prediction using machine learning,” 2014 IEEE Front. Educ. Conf. Proc., pp. 1–8, 2014.

[11] C. Sobie, C. Freitas, and M. Nicolai, “Simulation-driven machine learning: Bearing fault classification,” Mech. Syst. Signal Process., vol. 99, pp. 403–419, 2018.

[12] J. H. Lee, J. Shin, and M. J. Realff, “Machine learning: Overview of the recent progresses and implications for the process systems engineering field,” Comput. Chem. Eng., 2017.

[13] T. M. Mitchell, (Mcgraw-Hill International Edit) Thomas Mitchell-Machine learning-McGraw Hill Higher Education (1997). .

[14] S. RAY, “Understanding Support Vector Machine algorithm from examples,” 2017.

[15] A. M. Karim, Ö. Karal, and F. V Çelebi, “A New Automatic Epilepsy Serious Detection Method by Using Deep Learning Based on Discrete Wavelet Transform,” no. 4, pp. 15–18, 2018.

[16] A. M. Karim, Mehmet S. Güzel, Mehmet R. Tolun, Hilal Kaya, Fatih V. Çelebi, A new framework using deep auto-encoder and energy spectral density for medical waveform data classification and processing, Biocybernetics and Biomedical Engineering, Volume 39, Issue 1,2019,Pages 148-159, ISSN 0208-5216, https://doi.org/10.1016/j.bbe.2018.11.004.

[17] S. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. Chan, “Cost-based modeling for fraud and intrusion detection: results from the jam project, in: DARPA Information Survivability Conference and Exposition,” DISCEX’00, Proc., vol. 2, no. IEEE, 2000, pp. 130–144, 2000.

[18] M. Alkasassbeh, A. B. A. Hassanat, and G. Al-naymat, “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques,” vol. 7, no. 1, pp. 436–445, 2016.

[19] A. Abraham, C. Grosan, and C. Martin-Vide, “Evolutionary design of intrusion detection programs,” Int. J. Netw. Secur., vol. 4, no. 3, pp. 328–339, 2007.

[20] A. M. Brues, “Genetic effects of the atom bomb,” J. Hered., vol. 38, no. 5, pp. 137–137, 1947.

[21] H. Liu, Y. Sun, and M. S. Kim, “Fine-grained DDoS detection scheme based on bidirectional count sketch,” Proc. - Int. Conf. Comput. Commun. Networks, ICCCN, 2011.

[22] C. Khammassi and S. Krichen, “A GA-LR wrapper approach for feature selection in network intrusion detection,” Comput. Secur., vol. 70, pp. 255–277, 2017.

[23] A. Abraham and J. Thomas, “Distributed intrusion detection systems: a computational intelligence approach,” Idea Gr. Inc. Publ. Usa, Chapter, vol. 5, pp. 1–28, 2005.

[24] N. Sharma and S. Mukherjee, “A Novel Multi-Classifier Layered Approach to Improve Minority Attack Detection in IDS,” Procedia Technol., vol. 6, pp. 913–921, 2012.

[25] B. Škrbić and N. Durišić-Mladenović, “Principal component analysis for soil contamination with organochlorine compounds,” Chemosphere, vol. 68, no. 11, pp. 2144–2152, 2007.

[26] N. Patani and R. Patel, “A Mechanism for Prevention of Flooding based DDoS Attack,” vol. 13, no. 1, pp. 101–111, 2017.

[27] L. K. Xr et al., “8VLQJ 6WDFNHG ’ HQRLVLQJ $ XWRHQFRGHU IRU WKH,” pp. 483–488, 2017.

[28] Y. Feng, R. Guo, D. Wang, and B. Zhang, “Research on the active DDoS filtering algorithm based on IP flow,” 5th Int. Conf. Nat. Comput. ICNC 2009, vol. 4, no. October, pp. 628–632, 2009.

[29] A. Meek, “DDoS attacks are getting much more powerful and the Pentagon is scrambling for solutions,” 2015.

[30] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, p. 39, 2004.

[31] S. Taghavi Zargar, J. Joshi, D. Tipper, and S. Member, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” pp. 1–24, 2013.

[32] T. T. Oo and T. Phyu, “Analysis of DDoS Detection System based on Anomaly Detection System,” 2014.

[33] S. Sinha and M. Sharma, “Simulation and Analysis of DDoS Attacks by Specialized Simulator using Virtualization,” vol. 3, no. 2, pp. 2–4, 2014.

[34] Bojan Kolosnjaji, Apostolis Zarras, George Webster, and Claudia Eckert. Deep learning for classification of malware system call sequences. In Australasian Joint Conference on Artificial Intelligence, pages 137–149. Springer, 2016.

[35] B. Hang, R. Hu, and W. Shi, “An enhanced SYN cookie defence method for TCP DDoS attack,” J. Networks, vol. 6, no. 8, pp. 1206–1213, 2011.

[36] D. Wang, Z. Yufu, and J. Jie, “A multi-core based DDoS detection method,” Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010, vol. 4, pp. 115–118, 2010.

[37] Karim, A.M., Mishra, A. (2022). Novel COVID-19 Recognition Framework Based on Conic Functions Classifier. In: Garg, L., Chakraborty, C., Mahmoudi, S., Sohmen, V.S. (eds) Healthcare Informatics for Fighting COVID-19 and Future Epidemics. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-72752-9_1.

[38] J. Singh, M. Sachdeva, and K. Kumar, “Detection of DDoS Attacks Using Source IP Based Entropy,” vol. 3, no. 1, pp. 201–210, 2013.

[39] S. M. Lee, D. S. Kim, J. H. Lee, and J. S. Park, “Detection of DDoS attacks using optimized traffic matrix,” Comput. Math. with Appl., vol. 63, no. 2, pp. 501–510, 2012.

[40] H. Rahmani, N. Sahli, and F. Kamoun, “DDoS flooding attack detection scheme based on F-divergence,” Comput. Commun., vol. 35, no. 11, pp. 1380–1391, 2012.

[41] Senirkentli, Güler B., Fatih Ekinci, Erkan Bostanci, Mehmet S. Güzel, Özlem Dağli, Ahmad M. Karim, and Alok Mishra. 2021. "Proton Therapy for Mandibula Plate Phantom" Healthcare 9, no. 2: 167. https://doi.org/10.3390/healthcare9020167.

[42] S. M. Hosseini Bamakan, H. Wang, and Y. Shi, “Ramp loss K-Support Vector Classification-Regression; a robust and sparse multi-class approach to the intrusion detection problem,” Knowledge-Based Syst., vol. 126, pp. 113–126, 2017.

[43] Fatsuma Jauro, Haruna Chiroma, Abdulsalam Y. Gital, Mubarak Almutairi, Shafi’i

M. Abdulhamid, Jemal H. Abawajy, Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend, Applied Soft Computing, Volume 96, 2020, 106582, ISSN 1568-4946.

[44] A. M. Karim, F. V. Çelebi, and A. S. Mohammed, "Software Development for Blood Disease Expert System," Lecture Notes on Empirical Software Engineering, vol. 4, no. 3, pp. 179–183, 2016.

[45] A. M. Karim, M. S. Güzel, M. R. Tolun, H. Kaya, and F. V Çelebi, "A New Generalized Deep Learning Framework Combining Sparse Auto-encoder and Taguchi Method for Novel Data Classification and Processing," pp. 1–22.

[46] L. Wang, C. Wang, W. Du et al., "Parameter optimization of a four-legged robot to improve motion trajectory accuracy using signal-to-noise ratio theory," Robotics and Computer-Integrated Manufacturing, vol. 51, pp. 85–96, 2018..

[47] A. M. Karim, F. V. Çelebi, and A. S. Mohammed, "Software Development for Blood Disease Expert System," *Lecture Notes on Empirical Software Engineering*, vol. 4, no. 3, pp. 179–183, 2016.

[48] A. Karim, Development of secure Internet of Vehicle Things (IoVT) for smart transportation system, Computers and Electrical Engineering, Volume 102, 2022, 108101, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2022.108101.

[49] A. Mozaffer Karim, , Hilal Kaya, Veysel Alcan, Baha Sen, and Ismail Alihan Hadimlioglu. 2022. "New Optimized Deep Learning Application for COVID-19 Detection in Chest X-ray Images" *Symmetry* 14, no. 5: 1003. https://doi.org/10.3390/sym14051003.

[50] Z. Cui, Ruimin Ke, Ziyuan Pu, Yinhai Wang, Stacked bidirectional and unidirectional LSTM recurrent neural network for forecasting network-wide traffic state with missing values, Transportation Research Part C: Emerging Technologies, Volume 118, 2020, 102674, ISSN 0968-090X.

[51] Y. Chen, Voltages prediction algorithm based on LSTM recurrent neural network, Optik, Volume 220, 2020, 164869, ISSN 0030-4026.

[52] N. Andrei, A Dai–Yuan conjugate gradient algorithm with sufficient descent and conjugacy conditions for unconstrained optimization, Applied Mathematics Letters, Volume 21, Issue 2, 2008, Pages 165-171, ISSN 0893-9659.

[53] M. Maruf Öztürk, İbrahim Arda Cankaya, Deniz İpekçi, Optimizing echo state network through a novel fisher maximization based stochastic gradient descent, Neurocomputing, Volume 415, 2020, Pages 215-224, ISSN 0925-2312.

[54] A. Koreanschi, Oliviu Sugar Gabor, Joran Acotto, Guillaume Brianchon, Gregoire Portier, Ruxandra Mihaela Botez, Mahmoud Mamou, Youssef Mebarki, Optimization and design of an aircraft's morphing wing-tip demonstrator for drag reduction at low speed, Part I – Aerodynamic optimization using genetic, bee colony and gradient descent algorithms, Chinese Journal of Aeronautics, Volume 30, Issue 1, 2017, Pages

149-163, ISSN 1000-9361.

[55] A. Jentzen, Philippe von Wurstemberger, Lower error bounds for the stochastic gradient descent optimization algorithm: Sharp convergence rates for slowly and fast decaying learning rates, Journal of Complexity, Volume 57, 2020, 101438, ISSN 0885-064X, https://doi.org/10.1016/j.jco.2019.101438..

[56] R. Ye, Qun Dai, Implementing transfer learning across different datasets for time series forecasting, Pattern Recognition, Volume 109, 2021, 107617, ISSN 0031-3203,.

[57] Y. Liu, Ao Li, Xing-Ming Zhao, Minghui Wang, DeepTL-Ubi: A novel deep transfer learning method for effectively predicting ubiquitination sites of multiple species, Methods, 2020, ISSN 1046-2023,..

[58] J. Wu, Zhibin Zhao, Chuang Sun, Ruqiang Yan, Xuefeng Chen, Few-shot transfer learning for intelligent fault diagnosis of machine, Measurement, Volume 166, 2020, 108202, ISSN 0263-2241,..

[59] S. Wang, Lei Zhang, Jingru Fu, Adversarial transfer learning for cross-domain visual recognition, Knowledge-Based Systems, Volume 204, 2020, 106258, ISSN 0950-7051,..

[60] X. Yang, Yanfeng Zhang, Wei Lv, Dong Wang, Image recognition of wind turbine blade damage based on a deep learning model with transfer learning and an ensemble learning classifier, Renewable Energy, 2020, ISSN 0960-1481,..

[61] C. Li, Shaohui Zhang, Yi Qin, Edgar Estupinan, A systematic review of deep transfer learning for machinery fault diagnosis, Neurocomputing, Volume 407, 2020, Pages 121-135, ISSN 0925-2312,..

[62] Z. Qiu, Shutao Zhao, Xuping Feng, Yong He, Transfer learning method for plastic pollution evaluation in soil using NIR sensor, Science of The Total Environment, Volume 740, 2020, 140118, ISSN 0048-9697,

[63] Shanshan Wang, Lei Zhang, Jingru Fu, Adversarial transfer learning for cross-domain visual recognition, Knowledge-Based Systems, Volume 204, 2020, 106258, ISSN 0950-7051,..

[64] Xiyun Yang, Yanfeng Zhang, Wei Lv, Dong Wang, Image recognition of wind turbine blade damage based on a deep learning model with transfer learning and an ensemble learning classifier, Renewable Energy, 2020, ISSN 0960-1481,..

[65] Chuan Li, Shaohui Zhang, Yi Qin, Edgar Estupinan, A systematic review of deep transfer learning for machinery fault diagnosis, Neurocomputing, Volume 407, 2020, Pages 121-135, ISSN 0925-2312,..

[66] Yue Wang, Yuting Liu, Wei Chen, Zhi-Ming Ma, Tie-Yan Liu, Target transfer Q-learning and its convergence analysis, Neurocomputing, Volume 392, 2020, Pages 11-22, ISSN 0925-2312,..

[67] Zhengjun Qiu, Shutao Zhao, Xuping Feng, Yong He, Transfer learning method for plastic pollution evaluation in soil using NIR sensor, Science of The Total Environment, Volume 740, 2020, 140118, ISSN 0048-9697,..

[68] Santi Kumari Behera, Amiya Kumar Rath, Prabira Kumar Sethy, Maturity status classification of papaya fruits based on machine learning and transfer learning approach, Information Processing in Agriculture, 2020, ISSN 2214-3173,..

[69] Seunghyeon Kim, Yung-Kyun Noh, Frank C. Park, Efficient neural network compression via transfer learning for machine vision inspection, Neurocomputing, Volume 413, 2020, Pages 294-304, ISSN 0925-2312,..

[70] Xiang Li, Wei Zhang, Hui Ma, Zhong Luo, Xu Li, Partial transfer learning in machinery cross-domain fault diagnostics using class-weighted adversarial networks, Neural Networks, Volume 129, 2020, Pages 313-322, ISSN 0893-6080,..

[71] Piyush Kant, Shahedul Haque Laskar, Jupitara Hazarika, Rupesh Mahamune, CWT Based Transfer Learning for Motor Imagery Classification for Brain computer Interfaces, Journal of Neuroscience Methods, Volume 345, 2020, 108886, ISSN 0165-0270,..

[72] Xinghua Li, Zhongyuan Hu, Mengfan Xu, Yunwei Wang, Jianfeng Ma, Transfer learning based intrusion detection scheme for Internet of vehicles, Information Sciences, Volume 547, 2021, Pages 119-135, ISSN 0020-0255,..

[73] Sheikh Saud, Basharat Jamil, Yogesh Upadhyay, Kashif Irshad, Performance improvement of empirical models for estimation of global solar radiation in India: A k-fold cross-validation approach, Sustainable Energy Technologies and Assessments, Volume 40, 2020, 100768, ISSN 2213-1388,..

[74] Jie Wei, Hui Chen, Determining the number of factors in approximate factor models by twice K-fold cross validation, Economics Letters, Volume 191, 2020, 109149, ISSN 0165-1765.

[75] Tzu-Tsung Wong, Performance evaluation of classification algorithms by k-fold and leave-one-out cross validation, Pattern Recognition, Volume 48, Issue 9, 2015, Pages 2839-2846, ISSN 0031-3203,..

[76] Gaoxia Jiang, Wenjian Wang, Error estimation based on variance analysis of k-fold cross-validation, Pattern Recognition, Volume 69, 2017, Pages 94-106, ISSN 0031-320..

[77] Nima Shiri Harzevili, Sasan H. Alizadeh, Analysis and modeling conditional mutual dependency of metrics in software defect prediction using latent variables, Neurocomputing, Volume 460, 2021, Pages 309-330, ISSN 0925-2312, https://doi.org/10.1016/j.neucom.2021.05.043..

[78] Chao Ni, Xiang Chen, Fangfang Wu, Yuxiang Shen, Qing Gu, An empirical study on pareto based multi-objective feature selection for software defect prediction, Journal of Systems and Software, Volume 152, 2019, Pages 215-238, ISSN 0164-1212.

[79] Ruchika Malhotra, Shine Kamal, An empirical study to investigate oversampling methods for improving software defect prediction using imbalanced data, Neurocomputing, Volume 343, 2019, Pages 120-140, ISSN 0925-2312.

[80] Yerima, S. Y., Alzaylaee, M. K., & Sezer, S. (2019). Machine learning-based dynamic analysis of Android apps with improved code coverage. *EURASIP Journal on Information Security*, *2019*(1), 1-24.

[81] Siddiqui, M., Wang, M. C., & Lee, J. (2008, February). Data mining methods for malware detection using instruction sequences. In *Artificial Intelligence and Applications* (pp. 358-363).

[82] N. Milosevic, A. Dehghantanha, K-K. R. Choo. "Machine learning aided Android malware classification", Computers & Electrical Engineering, 61, 266-274, 2017.

[83] A. Pektaş, M. Çavdar, T. Acarman, "Android malware classification by applying online machine learning", (ISCIS 2016) International Symposium on Computer and Information Sciences, Kraków, Poland, 72-80, October 27–28, 2016.

[84] L. Onwuzurike, M. Almeida, E. Mariconti, J. Blackburn, G. Stringhini, E. D. Cristofaro, "A family of droids: Analyzing behavioral model based Android malware

detection via static and dynamic analysis", *arXiv:1803.03448*, https://arxiv.org/abs/1803. 03448, 2018.

[85] Xiangwen Wang, Xianghong Lin, Xiaochao Dang, Supervised learning in spiking neural networks: A review of algorithms and evaluations, Neural Networks, Volume 125, 2020, Pages 258-280, ISSN 0893-6080.

[86] Khalil Moshkbar-Bakhshayesh, Performance study of bayesian regularization based multilayer feed-forward neural network for estimation of the uranium price in comparison with the different supervised learning algorithms, Progress in Nuclear Energy, Volume 127, 2020, 103439, ISSN 0149-1970.

[87] Jiabin Zhang, Hu Su, Wei Zou, Xinyi Gong, Zhengtao Zhang, Fei Shen, CADN: A weakly supervised learning-based category-aware object detection network for surface defect detection, Pattern Recognition, Volume 109, 2021, 107571, ISSN 0031-3203.

[88]] Lu Han, Wenjun Li, Zhi Su, An assertive reasoning method for emergency response management based on knowledge elements C4.5 decision tree, Expert Systems with Applications, Volume 122, 2019, Pages 65-74, ISSN 0957-4174.

[89] X. Wang, C. Zhou, X. Xu, Application of C4.5 decision tree for scholarship evaluations, Procedia Computer Science, Volume 151, 2019, Pages 179-184, ISSN 1877-0509.

[90] Sunanda Gamage, Jagath Samarabandu, Deep learning methods in network intrusion detection: A survey and an objective comparison, Journal of Network and Computer Applications, Volume 169, 2020, 102767, ISSN 1084-8045.