ҒТАХР 81.93.29

10.51889/2959-5894.2025.89.1.019

Б. Омаров[1], А.Қ.Сердалы[1*], А.Ыдырыс[2], Б. Омаров[1,2]

[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан,
[2]Халықаралық Ақпараттық технологиялар университеті, Алматық., Қазақстан,
[*]*e-mail: altynayserdaly@gmail.com*

MINI-VGGNET НЕГІЗІНДЕГІ КОНВОЛЮЦИЯЛЫҚ НЕЙРОНДЫҚ ЖЕЛІЛЕР КӨМЕГІМЕН ЖЕЛІГЕ РҰҚСАТСЫЗ ЕНУДІ АНЫҚТАУ

Аңдатпа

Киберқауіптердің қарқынды өсуі және желілік трафиктің ұлғаюы жағдайында желілік шабуылдарды анықтау және алдын алу киберқауіпсіздікті қамтамасыз етудің өзекті міндеттеріне айналуда. Бұл зерттеудің мақсаты теңгерімсіз желілік трафиктегі ауытқуларды анықтау үшін тиімді Mini-VGGNet үлгісін әзірлеу болып табылады. Зерттеу сонымен қатар ықтимал қауіптерді дәлірек анықтауға мүмкіндік беретін деректердегі уақытқа тәуелділікті талдауға бағытталған. Жұмыста желілік деректерден белгілерді алу үшін конволюциялық қабаттар мен пулинг қабаттарын қамтитын mini-VGGNet архитектурасына негізделген терең оқыту әдістемесі қолданылады. Анықтау тиімділігін арттыру үшін деректерді өңдеу әдістері қолданылады, соның ішінде қажет емес мәндерді жою және қалыпқа келтіру, бұл модельдің оқу сапасын жақсартады. Модель нақты уақыттағы ауытқуларды анықтауға және желілік трафиктің өзгеруіне бейімделуге мүмкіндік беретін желілік шабуылдардың әртүрлі түрлерін қамтитын деректер жиынтығында оқытылады. Зерттеу нәтижесінде ұсынылған модельдің тиімділігін растайтын желілік интрузияларды анықтауда жоғары дәлдікке қол жеткізілді. Нәтижелер Mini-VGGNet моделі ауытқуларды анықтау жылдамдығы мен дәлдігіне қатысты дәстүрлі әдістерден айтарлықтай жоғары екенін көрсетеді. Жұмыстың маңыздылығы оның киберқорғау әдістерін дамытуға және үнемі өзгеріп отыратын киберқауіптер жағдайында аса маңызды болып табылатын ақпараттық жүйелердің қауіпсіздік деңгейін арттыруға қосқан үлесі болып табылады. Нәтижелер киберқауіпсіздікті одан әрі зерттеу және желілік шабуылдарды анықтау үшін жетілдірілген модельдерді әзірлеу үшін пайдаланылуы мүмкін.

Түйін сөздер: нейрондық желі, терең оқыту, intrusion detection system, Mini-VGGNet, теңгерімсіз деректер, CICIDS2017 деректер жиынтығы.

Б. Омаров[1], А.К.Сердалы[1], А.Ыдырыс[2], Б. Омаров[1,2]
[1] Казахский национальный университет им. Аль-Фараби, г.Алматы, Казахстан,
[2] Международный университет информационных технологий, г.Алматы, Казахстан

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ СВЁРТОЧНОЙ НЕЙРОННОЙ СЕТИ НА ОСНОВЕ MINI-VGGNET

Аннотация

В условиях стремительного роста киберугроз и увеличения объема сетевого трафика, выявление и предотвращение сетевых вторжений становятся актуальными задачами для обеспечения кибербезопасности. Целью данного исследования является разработка эффективной модели Mini-VGGNet для обнаружения аномалий в несбалансированном сетевом трафике. Исследование также направлено на анализ временных зависимостей в данных, что позволяет более точно идентифицировать потенциальные угрозы. В работе используется методология глубокого обучения, основанная на архитектуре Mini-VGGNet, которая включает конволюционные слои и пулинг-слои для извлечения признаков из сетевых данных. Для повышения эффективности обнаружения применяются методы предобработки данных, включая удаление ненужных значений и нормализацию, что улучшает качество обучения модели. Модель обучается на наборе данных, содержащем различные типы сетевых атак, что позволяет выявлять аномалии в реальном времени и адаптироваться к изменениям в сетевом трафике. В результате проведенного исследования достигнута высокая точность в обнаружении сетевых вторжений, что подтверждает эффективность предложенной модели. Полученные результаты показывают, что модель Mini-VGGNet значительно превосходит традиционные методы в отношении

скорости и точности обнаружения аномалий. Значимость работы заключается в ее вкладе в развитие методов киберзащиты и повышении уровня безопасности информационных систем, что является критически важным в условиях постоянно изменяющихся киберугроз. Результаты могут быть использованы для дальнейших исследований в области кибербезопасности и разработки более продвинутых моделей для обнаружения сетевых атак.

Ключевые слова: нейронная сеть, глубокое обучение, intrusion detection system, Mini-VGGNet, несбалансированные данные, набор данных CICIDS2017.

B. Omarov[1], A. Serdaly[1], A. Ydyrys[2], B. Omarov[1,2]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan,
[2]International Information Technology University, Almaty, Kazakhstan

INTRUSION DETECTION USING MINI-VGGNET-BASED CONVOLUTIONAL NEURAL NETWORK

Abstract

In the context of the rapid growth of cyber threats and an increase in the volume of network traffic, the detection and prevention of network intrusions are becoming urgent tasks to ensure cybersecurity. The purpose of this study is to develop an effective Mini-VGGNet model for detecting anomalies in unbalanced network traffic. The study also aims to analyze time dependencies in the data, which allows for more accurate identification of potential threats. The work uses a deep learning methodology based on the Mini-VGGNet architecture, which includes convolution layers and pooling layers to extract features from network data. To improve detection efficiency, data preprocessing methods are used, including removing unnecessary values and normalization, which improves the quality of model training. The model is trained on a dataset containing various types of network attacks, which allows you to identify anomalies in real time and adapt to changes in network traffic. As a result of the conducted research, high accuracy in detecting network intrusions has been achieved, which confirms the effectiveness of the proposed model. The results show that the Mini-VGGNet model is significantly superior to traditional methods in terms of speed and accuracy of anomaly detection. The significance of the work lies in its contribution to the development of cyber defense methods and improving the security of information systems, which is critically important in the context of constantly changing cyber threats. The results can be used for further research in the field of cybersecurity and the development of more advanced models for detecting network attacks.

Keywords: neural network, deep learning, intrusion detection system, Mini-VGGNet, imbalanced data, CICIDS2017 dataset.

Негізгі ережелер

Ұсынылған Mini-VGGNet-Intrusion моделі, әсіресе теңгерімсіз деректер жағдайында, желіге рұқсатсыз енуді анықтауда айтарлықтай жетістіктер мен нәтижелер көрсетті. Оның конволюциялық қабаттарға негізделген архитектурасы шабуылдардың көптеген түрлері үшін жоғары жіктеу дәлдігін қамтамасыз етеді, бұл оны нақты желіге рұқсатсыз енуді анықтау және алдын алу жүйелерінде (IDS/IPS) қолдануға мүмкіндік береді. Бұл архитектура 15 түрлі шабуыл класстарын, оның ішінде DoS және DDoS сияқты шабуылдарды дәл анықтауға арналған. Ұсынылған терең оқыту моделі Mini-VGGNet-Intrusion дәлдігі 0.985 көрсеткішіне ие.

Кіріспе

Ақпараттық технологиялардың қарқынды дамуы және желілік трафиктің ұлғаюы жағдайында киберқауіпсіздік бүкіл әлемдегі ұйымдар үшін басты міндеттердің біріне айналуда. Желілік шабуылдар деректердің бұзылуын, қаржылық шығындарды және маңызды жүйелердің дұрыс жұмыс істемеуін қоса алғанда, ауыр зардаптарға әкелуі мүмкін. Желілік шабуылдарды тиімді анықтау және алдын алу ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін басымдық болып табылады. Киберқылмыспен күресудің негізгі әдістері антивирустық бағдарламалық жасақтама, брандмауэр және желіге рұқсатсыз енуді анықтау жүйелері (IDS) болып табылады [1]. Желіге рұқсатсыз енуді анықтау жүйесі (IDS) – рұқсат

етілмеген немесе зиянды әрекеттерді анықтау мақсатында желілік трафик пен хост әрекеттерін бақылауға арналған құрал. IDS екі түрлі болуы мүмкін: белгілі бір құрылғыдағы әрекеттерді басқаратын HEADS және нақты уақыт режимінде желілік трафикті бақылайтын NIDS. Шабуылдарды анықтау үшін IDS қолтаңбаға негізделген әдістерді (белгілі шабуыл үлгілерін табу) және ауытқуларды (қалыпты мінез-құлықтан ауытқуларды анықтау) пайдаланады. IDS-тің негізгі мәселелеріне жалған позитивтер және жаңа шабуылдарды анықтаудағы қиындықтар жатады. Машиналық және терең оқытуды қолдануды қамтитын заманауи тәсілдер мұндай жүйелердің дәлдігі мен бейімделуін жақсартуға көмектеседі, әсіресе теңгерімсіз деректер жағдайында [2].

Желілік шабуылдарды анықтау мәселелеріндегі маңызды мәселелердің бірі-деректердің теңгерімсіздігі. Нақты сценарийлерде желілік трафик көп жағдайда қалыпты деректерді білдіреді, ал шабуыл жағдайлары әлдеқайда сирек кездеседі. Желілік шабуылдарды анықтаудың заманауи тәсілдері бұл мәселені шешу үшін терең оқыту әдістерін көбірек қолданады. LSTM және CNN сияқты терең нейрондық желілер желілік деректердегі күрделі үлгілерді анықтауға және қалыпты трафикті де, шабуылдардың әртүрлі түрлерін де тиімді жіктеуге қабілетті. Дегенмен, терең модельдерді пайдаланғанның өзінде, теңгерімсіз деректер мәселесі өзекті болып қала береді, анықтаудың жоғары дәлдігін қамтамасыз ету үшін қосымша әдістерді қолдануды талап етеді [3]. Соңғы жылдары желілік шабуылдарды анықтау үшін терең нейрондық желілерді қолдануға қызығушылық артып келеді. Зерттеулер көрсеткендей, конволюциялық нейрондық желілер (CNN) және ұзақ мерзімді жады (LSTM) желілері сияқты архитектуралар дәстүрлі әдістермен салыстырғанда жақсартылған нәтижелерді көрсетеді. Дегенмен, тіпті терең оқытудың озық тәжірибелері теңгерімсіз деректер мәселесіне тап болады, бұл олардың нақты сценарийлердегі өнімділігін жақсарту үшін қосымша зерттеулер мен жаңа тәсілдерді әзірлеуді қажет етеді.

Терең оқыту және нейрондық желі архитектурасы. Терең оқыту қабаттарға біріктірілген жасанды нейрондардан тұратын жасанды нейрондық желілерге қолданылады. Мұндай желіде кіріс деректері кіріс деп аталатын бірінші қабаттан аралық (жасырын) қабаттар арқылы соңғы (шығыс) қабатқа өту процесінде өңделеді. Егер аралық қабаттар біреуден көп болса, мұндай жасанды нейрондық желі терең деп аталады. Нейрондар ұсынылатын функция активтендіру функциясы деп аталады. Активтендіру функциясының мәні нейрон кірістерінің өлшенген қосындысына және шекті мәнге байланысты, нейронның шығысы активтендіру функциясын кіріс векторының скалярлық көбейтіндісіне және берілген қашықтыққамещысқан Нейрон салмағының векторына қолдану нәтижесі болып табылады [4]. Активтендіру функциясы ретінде қолданылатын сызықтық емес функциялардың мысалдары-сигмоид, softmax функциясы, сызықтық түзеткіш (rectified linear unit, ReLU), гиперболалық тангенс. Нейрондық желіні оқыту мақсатты айнымалының дұрыс мәні мен нейрондық желі болжаған мән арасындағы айырмашылықты сипаттайтын жоғалту (қате) функциясын пайдаланады. Нейрондардың, қабаттардың, олардың өзара байланыстарының әртүрлі конфигурациялары нейрондық желілердің әртүрлі архитектураларын тудырады. Терең оқыту әдістерін осылайша қолданылатын нейрондық желі архитектурасы бойынша жіктеуге болады. Әрі қарай, сәйкес жұмыстарды талдауда пайда болатын терең оқытудың негізгі әдістерінің қысқаша сипаттамасы келтірілген.

Жасанды нейрондық желі (Artificial Neural Network, ANN), жоғарыда айтылғандай, жасырын қабаттардың санына байланысты терең (deep Neural Network, DNN) және таяз (Shallow Neural Network, s-NN) болуы мүмкін. Мұндай желілердің негізгі нұсқасы-тікелей тарату желісі (feed forward neural network), онда сигнал кіруден шығысқа қарай қатаң түрде таралады. Оқыту әдетте қатені кері тарату әдісімен жүзеге асырылады. Көп қабатты перцептрон (Multilayer Perceptron, MLP) – Ф.Розенблатт ұсынған мидың ақпаратты қабылдауының математикалық моделіне негізделген нейрондық желілердің қарапайым түрі-перцептронның бір түрі [5]. MLP-бұл кіріс және шығыс қабаттары арасында бір немесе бірнеше жасырын қабаттар болуы мүмкін толық байланысқан ANN [6].

Конволюциялық нейрондық желі (Convolutional Neural Network, CNN) - ауыспалы конволюциялық (convolution layers) және субдиск (subsampling layers немесе pooling layers) қабаттары бар бір бағытты көп қабатты желі. Конволюциялық қабат салмақ матрицасын (конволюция ядросы) кіріс қабатының әрбір фрагментіне элементтік көбейту және шығыс қабатының ұқсас позициясына жазылатын нәтижені қосу арқылы белгілер картасын құрайды. CNN бастапқыда кескіндерді өңдеу үшін қолданылған, бірақ қазіргі уақытта басқа тапсырмаларда да қолданылады. Желіге рұқсатсыз енуді анықтау мәселесіне қолдану тұрғысынан бұл деректер жиынындағы әрбір ерекшелік векторын "тор" немесе кесте пішімі бар шартты "кескінге" түрлендіріп, қалыпқа келтіру керек дегенді білдіреді [7].

Қайталанатын нейрондық желі (recurrent Neural Network, RNN) - нейрондар арасындағы байланыстар ішкі жады бар және деректерді өздеріне жібере алатын бағытталған тізбекті құрайтын желі. Мұндай желі архитектурасы RNN-ге уақыт бойынша динамикалық мінез-құлыққа ие болуға мүмкіндік береді және ерікті ұзындықтағы дәйекті деректерді өңдеу мүмкіндігін анықтайды. Қайталанатын нейрондық желі мұғалімді тартудың әртүрлі деңгейлерімен оқытылуы мүмкін, оның түрлері – төменде сипатталған LSTM және GRU. Қысқа мерзімді жад элементтерінің ұзын тізбегі (Long Short-Term Memory, LSTM) RNN-ге тән жойылып бара жатқан градиент мәселесін шешуге арналған. LSTM-де деректерді сақтау активтендіру функциясын жүзеге асыратын арнайы құрылымдар-"қақпалар" немесе "қақпалар" (gates) бар жад ұяшығы болып табылатын қайталанатын LSTM модулімен қамтамасыз етіледі. LSTM модулі қысқа және ұзақ уақыт аралығында мәндерді есте сақтауға мүмкіндік береді. Басқарылатын қайталанатын блок немесе нейрон (Gated Recurrent Unit, Gru) LSTM тәрізді ұяшық опциясын пайдаланады, бірақ "қақпалары"аз. Осылайша, GRU LSTM-ге қарағанда аз параметрлерге ие және оқыту үшін аз ресурстарды қажет етеді. Екі бағытты GRU (Bidirectional gru, BGRU) және екі бағытты LSTM (bidirectional LSTM, BiLSTM) сәйкесінше Gru және LSTM түрлері болып табылады, бұл желіге тек өңделген деректерге ғана емес, сонымен бірге бүкіл тізбекке негізделген нәтижені болжауға мүмкіндік береді. Мұндай желілерде есептеудің екі бағыты бар: нейрондардың Шығыс блоктары өткенге де, болашаққа да байланысты көріністі есептейді [8].

Әдебиеттік шолу

Бұл бөлімде сәйкес жұмыстарды талдау және оларда сипатталған терең оқыту әдістерін салыстыру берілген. Осы жұмыста талданған зерттеулердің көпшілігі Google Scholar [9] базасынан "Publish or Perish" [10] бағдарламасының көмегімен таңдалды.

[11] жұмыста желіге рұқсатсыз енуді анықтау мәселесін шешу үшін CNN-BiLSTM қолданылады: CNN кеңістіктік белгілерді, BiLSTM уақытша белгілерді анықтайды. Гибридті іріктеу (SMOTE-пен бірге OSS) оқу уақытын азайту және деректер жиынтығын теңестіру үшін қолданылады. Гибридті іріктеуден кейін барлық салыстырылған модельдер үшін оқу уақыты қысқарды, CNN-BiLSTM LeNet-5 оқу жылдамдығынан төмен болды, бірақ барлық басқа көрсеткіштер бойынша жақсы нәтиже көрсетті. Салыстыру NSL-KDD және UNSW-NB15 деректер жиынтығында жүргізілген.

[12] мақалада желіге рұқсатсыз енуді анықтау мәселесін шешуде 3 жасырын қабаты бар терең нейрондық желі (DNN) классикалық машиналық оқыту алгоритмдерімен салыстырғанда жақсы нәтиже көрсетті. Салыстыру DNN үшін KDD Cup 99 деректер жиынтығында 1-5 жасырын қабаттармен және Ada Boost, Decision Tree, K-Nearest Neighbor, Linear Regression, Navie Bayes, Random Forest, SVM*-Linear, SVM*-rbf алгоритмдерімен жүргізілді. Алайда, авторлар қазіргі заманғы деректер жиынтығында және нақты жағдайларда, соның ішінде қарсылас ортада (adversarial environment) зерттеулер жүргізу қажет екенін атап өтті.

Келесі жұмыста [13] желіге рұқсатсыз енуді анықтау тапсырмасы үшін конволюциялық қайталанатын нейрондық желіге негізделген гибридті IDS әзірленді: CNN кеңістіктік белгілерді, RNN уақытша белгілерді анықтайды. Деректер теңгерімсіздігінен құтылу үшін

миноритарлық класс мысалдарының көшірмесі (oversampling) қолданылды. Өнімділікті бағалау үшін нейрондық желі CNN және RNN қабаттарының алдына жалпылау қабілетін жақсарту және нейрондық қайта оқытуды азайту үшін Гаусс Шу қабаттары қосылды. Тиімділікті бағалау CSE-CIC-IDS2018 деректер жинағында жүргізілді: авторлар жүргізген әдістерді салыстыру да, басқа зерттеулердің деректері де пайдаланылды. Осы зерттеуде жүргізілген экспериментте ұсынылған модель шешім ағашымен, логистикалық регрессиямен және XGBoost алгоритмімен салыстырғанда жақсы нәтиже көрсетті. Айта кету керек, бұл зерттеу екі түрлі салыстыруды ұсынғанымен, әртүрлі бағалау жиынтықтары қолданылады және оларда көрсетілген ұпайлар сәйкес келмейді.

[14] зерттеуде желіге рұқсатсыз енуді анықтау мәселесін шешу үшін деректерді векторлық форматтан "кескінге" (матрицаға) алдын-ала түрлендіре отырып, CNN қолданылады. Белгілер кеңістігінің өлшемін азайту үшін негізгі компоненттер әдісі (PCA) және автокодер (AE) қолданылды, оқытуды оңтайландыру үшін пакеттік қалыпқа келтіру (batch normalization, BN) қолданылды. Дәстүрлі Машиналық оқыту алгоритмдерімен (Naive Bayes, Logistic Regression, Decision Tree, Random Forest, SVM, Adaboost), RNN және үш қабатты DNN-мен салыстырғанда, ұсынылған модель анықтау уақытын едәуір қысқартады және KDD Cup 99 деректер жиынтығында жақсы нәтиже көрсетеді. Дегенмен, модель пайдаланылған деректер жиынында осы шабуылдардың мысалдарының аздығына байланысты User to Root (U2R) және Remote to Local (R2L) типтерінің шабуылдарын анықтаудың төмен деңгейін көрсетеді – сәйкесінше 20.61% және 18.96%. Әрі қарайғы зерттеулерде авторлар бұл мәселені генеративті-қарсылас желі (GAN) көмегімен шабуыл мысалдарын құру арқылы шешуді жоспарлап отыр.

[15] мақалада желіге рұқсатсыз енуді анықтау мәселесін шешу үшін NSL-KDD деректер жиынтығынан деректерді екілік векторларға түрлендіру әдісі ұсынылған, олардан CNN көмегімен жіктеу үшін "кескін" (матрица) жасалады, бұл белгілерді таңдау кезеңін болдырмайды. NSL-KDD түрлендірілген деректер жиынтығының ішкі жиындарында сыналған CNN желілері (ResNet 50 және GoogLeNet) стандартты классификаторларға қарағанда жақсы нәтиже көрсетті, бірақ state-of-art шешімдерінен онша жақсы емес (салыстыру j48, Naive bayes, NB Tree, Random forest, Random tree, Multi-layer perceptron, SVM әдістерімен болды).

[16] жұмыста желіге рұқсатсыз енуді анықтау мәселесін шешу үшін қайталанатын нейрондық желілерді (RNN) пайдалану ұсынылады. Екілік және көп класты жіктеу үшін RNN NSL-KDD деректер жиынындағы дәстүрлі алгоритмдерге (J48, ANN, RF, SVM және т.б.) қарағанда өнімділікті жақсырақ көрсетеді, бірақ оқуға көп уақыт кетеді. Ұсынылған әдіс сонымен қатар KDD CUP 1999 деректер жинағындағы кішірейтілген RNN [17] қарағанда жақсы нәтижелерді көрсетеді. Мақалада сонымен қатар гиперпараметрлерді таңдау қарастырылады: нейрондар саны мен оқу жылдамдығының әдіс дәлдігіне әсері. Бұл жұмыстың авторлары осы әдістің жойылып кету және жарылу градиенттерінің проблемаларын атап өтеді және осы мәселелерді шешу үшін LSTM және Bidirectional RNN-ді одан әрі зерттеуді ұсынған.

[18] мақалада жасанды нейрондық желілерді корреляцияға негізделген белгілерді таңдаумен біріктіретін желіге рұқсатсыз енуді анықтау моделі ұсынылған (Correlation based Feature Selection, CFS). Модель RapidMiner құралының көмегімен жүзеге асырылды және NSL-KDD және UNSW-NB15 деректер жиынтығында тексерілді. CFS пайдалану деректердің өлшемін азайту арқылы модельдің дәлдігін, ерекшелігі мен сезімталдығын арттыруға, есептеу уақытын қысқартуға мүмкіндік берді. Іске асырылған модельді басқа заманауи тәсілдермен салыстыру жүргізілді: бұл модель жақсы нәтиже көрсетеді, бірақ көп есептеу уақытын қажет етеді. Ұсынылған тәсілді әртүрлі байланыс желілерінде, заттар интернетінің серверлерін қорғау үшін қолдануға болады (Internet of Things, IoT).

[19] мақалада желіге рұқсатсыз енуді анықтау мәселесін шешу үшін екі нейрондық желіден тұратын модель ұсынылған: Shallow Neural Network (S-NN) және Deep-Optimized Neural Network (DONN). S-NN желісі қарапайым және жылдам, D-ONN күрделі және баяу. Белгілерді таңдау корреляциялық талдау әдісімен және энтропиялық тәсілді қолдану арқылы жүзеге

асырылды. Бұл модель KDD Cup 99 деректер жиынтығында жақсы нәтиже көрсетті. Авторлар бұл әдісті сымсыз желілер мен IoT қорғау үшін қолдану мүмкіндігін атап өтеді.

Келесі мақалада [20] желіге рұқсатсыз енуді анықтау мәселесін шешу үшін BGRU+MLP моделі ұсынылған. Эксперименттерде KDD Cup 99 және NSL-KDD деректер жиынтығы қолданылды. Тәжірибе нәтижелері бойынша GRU LSTM – ге қарағанда жақсы нәтиже көрсетеді, BGRU-жеке GRU-ға қарағанда жақсы, ал BGRU мен MLP комбинациясы RNN (GRU немесе LSTM) немесе MLP-ді жеке қолданумен салыстырғанда жақсы нәтиже береді. BGRU+MLP дәлдігі, анықталған оқиғалардың саны және жалған оң мысалдардың (FPR) үлесі бойынша жақсы нәтижелерді көрсетеді, бірақ R2L және U2R типті шабуылдарды анықтауда қиындықтар бар. Авторлар бұл мәселе пайдаланылған деректер жиынындағы шабуылдардың аздығына байланысты басқа зерттеушілер жүйелеріне де тән екенін атап өтті.

[21] зерттеуде желіге рұқсатсыз енуді анықтау мәселесін шешу үшін SFSDT+RNN моделі ұсынылған. Бұл модель шабуылдарды, соның ішінде шабуылдардың жекелеген түрлерін анықтау дәлдігін жақсартуға арналған-атап айтқанда, бұрын айтылған R2L және U2R. Ерекшеліктерді таңдау үшін SFSDT гибридті алгоритмі қолданылады: дәйекті тікелей таңдау алгоритмі (SFS) көмегімен белгілердің ең маңызды жиынтығы таңдалады, олардың арасында шешім қабылдау ағашының көмегімен белгілердің ең жақсы жиынтығы анықталады (DT). Тәжірибелер NSL-KDD және ISCX 2012 деректер жиынтығында жүргізілді. LSTM-ді қолданатын Модель RNN-дің үш түрінің (RNN, LSTM, GRU) ең жақсы дәлдігін көрсетті. SFSDT көмегімен белгілерді таңдау арқылы есептеу уақыты мен жадты пайдалану азайды. Айта кету керек, бұл зерттеуде эксперименттерде қолданылатын архитектуралардың (RNN, LSTM, GRU) нақты іске асырылуының егжей-тегжейлері көрсетілмеген. IDS-те терең оқытуды қолдану саласындағы аналитикалық шолулар болып табылатын зерттеулерге ерекше назар аударған жөн.

[22] мақалада 2015-2019 жылдардағы IDS-те нейрондық желілерді пайдалану туралы әдебиеттерге шолу берілген. Зерттеуге әдебиеттерге шолулар, жаңа әдістер бойынша ұсыныстар және оқу мақалалары кірді. Нейрондық желі архитектурасының шабуылдарды анықтау жүйелерінде ең көп қолданылатын мәліметтер жиынтығы, жалпы және жеке мәліметтер жиынтығы, оларды пайдалану ерекшеліктері қарастырылады. IDS-те нейрондық желілерді пайдалану кезінде қауіпсіздік салдары мәселесі көтеріледі.

Келесі жұмыста [23] авторлар ұсынған IDS таксономиясы тұрғысынан IDS-те машиналық оқыту мен нейрондық желілерді пайдалану туралы әдебиеттерге шолу жасалады. Зерттеуге IDS-те жиі қолданылатын машиналық оқыту алгоритмдері, көрсеткіштері, деректер жиыны бойынша IDS классификацияларына шолулар кірді. Пәндік саладағы проблемалар мен болашақ зерттеу бағыттары атап өтілді.

Зерттеулерде [24] киберқауіпсіздік міндеттері үшін терең оқытудың аналитикалық шолуы ұсынылған. Киберқауіпсіздіктің нақты қосымшасына байланысты әр түрлі терең оқыту әдістерін қолдану қарастырылады. Авторлар киберқауіпсіздік міндеттерінде терең оқыту әдістерін қолданудың қолданылуы мен ерекшеліктері туралы қорытынды жасады.

1 - кестеде желіге р ұқсатсыз енуді анықтау тапсырмасы үшін терең оқыту әдістерін қолдану бойынша ғылыми зерттеу жұмыстарына талдау жасалды.

Жұмыстың жартысына жуығы нейрондық желі әдістермен қолданылады. Бұл әдістер белгілерді жобалау үшін қолданылады (қолтаңба кеңістігін бөлуге немесе азайтуға арналған), оқу процесін оңтайландыру (мысалы, деректер жиынтығын теңестіру немесе қайта оқытуды азайту әдістері), жіктеу. Әртүрлі түрлері бар RNN және CNN жиі кездеседі.

Әр түрлі архитектуралардың бір әдіспен үйлесуі белгілі бір әдістердің кемшіліктерін жоюға немесе жалпы шабуылдарды анықтаудың бүкіл процесін автоматтандыру дәрежесін жақсартуға арналған. Зерттеушілер белгілерді жобалау әдістеріне, деректерді өңдеуге немесе әртүрлі көмекші әдістерге (мысалы, оңтайландыру әдістері) назар аударатын жұмыстардың басым болуы зерттеулерде алынған жоғары нәтижелерге нейрондық желілердің қол жеткізуі үшін берілген қадамдардың маңыздылығы туралы айтуға мүмкіндік береді.

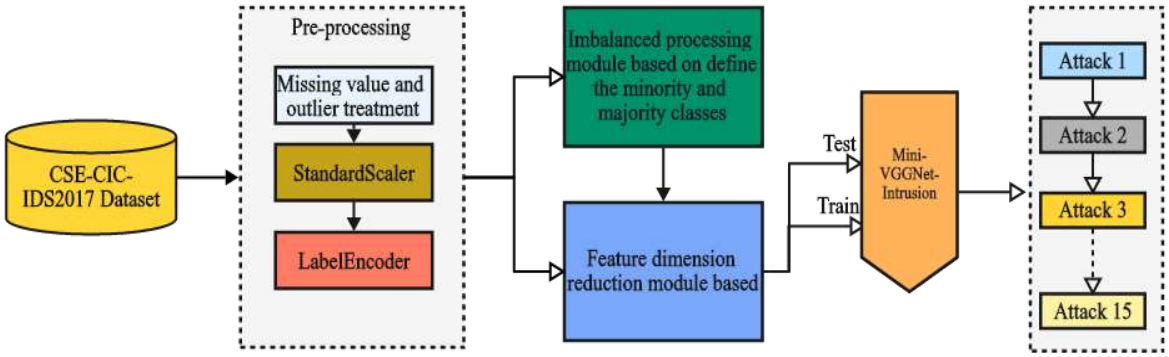
Кесте 1. Ғылыми зерттеу жұмыстарына талдау.

№	Ғылыми зерттеу жұмысы	Қолданылған әдістер	Мәлеметтер қоры	Бағалау
1.	K. Jiang және басқалары, 2020 [11] Тілі ағылшын	CNN-BiLSTM	NSL-KDD	ACC=83.58, Precision= 85.82, Recall=84.49, F1=85.14
			UNSW-NB15	ACC=77.16, Precision=82.63 , Recall=79.91, F1=81.25
2.	Rahul Vigneswaran және басқалары, 2018 [12]	DNN	KDD CUP 1999	DNN (3 қабат): ACC=93, Precision=99.7, Recall=91.5, F1=95.5
3.	M.A. Khan, 2021 [13] Тілі ағылшын	HCRNN (CNN-RNN)	CSE-CIC-IDS 2018	ACC=97.75, Precision= 0.9633, Recall=0.9712, F1=0.976, DR=0.97, FAR=2.5
4.	Yihan Xiao және басқалары, 2019 [14] Тілі ағылшын	CNN	KDD CUP 1999	ACC= 94, DR=93, FAR=0.5
5.	Zhipeng Li және басқалары, 2017 [15] Тілі ағылшын	CNN	NSL-KDD Test+	ResNet50: ACC=79.14, Precision= 91.97, Recall=69.41, F1=79.12 GoogLeNet: ACC=77.04, Precision= 91.66, Recall=65.64,
			NSL-KDD Test−21	ResNet50: ACC=81.57, Precision= 81.81, Recall=99.63, F1=89.85 GoogLeNet: ACC=81.84, Precision= 81.84, Recall=100, F1=90.01
6.	C. Yin және басқалары, 2017 [16] Тілі ағылшын	RNN	NSL-KDD деректер жинағы	ACC=83.28
7.	Sumaiya Thaseen және басқалары, 2020 [18] Тілі ағылшын	CFS + ANN	NSL-KDD	ACC=97.49, Specificity=99.3 1
			UNSW-NB15	ACC=96.44, Specificity=98.4
8.	Mangayarkarasi Ramaiah және басқалары, 2021 [19] Тілі ағылшын	Shallow Neural Network Model (S-NN), DeepOptimized Neural Network Model (D-ONN)	KDD CUP 1999	S-NN: ACC=91, Precision=93, Recall=93 D-ONN: ACC=98, Precision=93, Recall=93, F1=98
9.	Congyuan Xi және басқалары, 2018 [20] Тілі ағылшын	BGRU + MLP	KDD CUP 1999	ACC=99.84, DR=99.42, FPR=0.05
			NSL-KDD	ACC=99.24, DR=99.31, FPR=0.84
10.	Thi-Thu-Huong Le және басқалары, 2019 [21] Тілі ағылшын	SFSDT + RNN (RNN, LSTM, GRU)	NSL-KDD	RNN: ACC=89.6 LSTM: ACC=92 GRU: ACC=91.8
			ISCX 2012	RNN: ACC=94.75 LSTM: ACC=97.5 GRU: ACC=97.08

Қарастырылған зерттеулерде жүргізілген эксперименттерде ұсынылған терең оқыту әдістерін салыстыру негізінен басқа терең оқыту әдістерімен (соның ішінде ұсынылған әдістің өзгеруімен) немесе машиналық оқытудың әртүрлі әдістерімен жүзеге асырылады. Әдістерді салыстыру көбінесе KDD Cup 1999 және NSL-KDD 2009, UNSW-NB15 және ISCX 2012 деректер жиынтығында жүргізілді. Талданған зерттеулердегі ең заманауи деректер жиынтығы-CSECIC – IDS2018. Машиналық оқытудың классикалық әдістеріне тән терең оқыту әдістерінің проблемасын атап өткен жөн: оларды оқыту үшін қазіргі заманғы деректерге сәйкес келмейтін ескірген теңгерімсіз деректер жиынтығын пайдалану. Қарастырылған зерттеулерде желіге рұқсатсыз енуді анықтау тапсырмасы үшін терең оқыту әдістерін қолдану көбінесе көп класты жіктеу тапсырмасы үшін жүзеге асырылады. Сапаны бағалау үшін барлық зерттеулер дұрыс жауаптардың үлесін пайдаланады (accuracy, ACC) және сапаны бағалаудың басқа жиі кездесетін көрсеткіштері-жұмыстың жартысына жуығында кездесетін дәлдік (дәлдік), толықтық (қалпына келтіру), F-Өлшем (F1) және анықтау жиілігі (DR) қолданылған.

Зерттеу әдіснамасы

1-суретте ұсынылған модельдің құрылымы үш негізгі модульден тұрады: теңгерімсіздікті өңдеу модулі, объектілерді кішірейту модулі және жіктеу модулі. Әрбір модуль гиперпараметрлік іздеу арқылы тәжірибе мен көптеген эксперименттер негізінде оңтайландырылған, бұл жақсы нәтиже алуды қамтамасыз етеді.



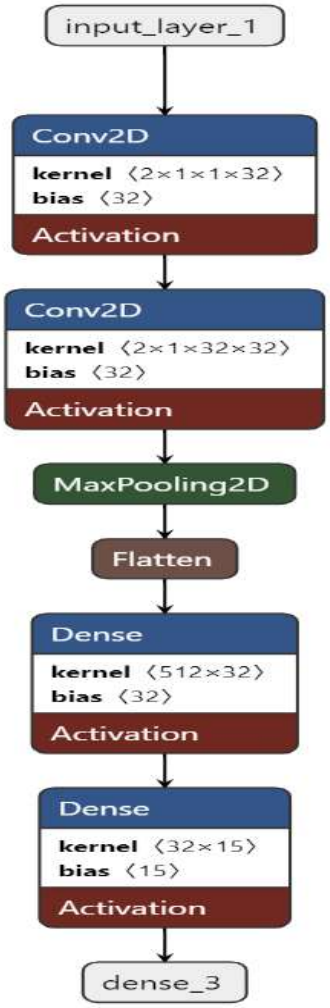
Сурет 1. Модельдің құрылымы

Теңгерімсіз деректерді қолдана отырып, желілік шабуылдарды анықтау міндеті үшін CICIDS2017 деректер жиынтығында MINI-VGGNet архитектурасына негізделген модель жасалды. CICIDS2017 — желілік шабуылдарды анықтауға арналған кеңінен қолданылатын деректер жинағы. Бұл жинақ 2017 жылы Канададағы Киберқауіпсіздік зерттеу орталығы (Canadian Institute for Cybersecurity) тарапынан жасалған. CICIDS2017 нақты әлемдік желілік трафикті имитациялайды және түрлі шабуылдардың кең спектрін қамтиды, соның ішінде DoS, DDoS, PortScan, Brute Force, XSS, SQL Injection және басқалар. Деректер жинағында трафиктің әртүрлі түрлері және BENIGN деп белгіленген қауіпсіз трафик бар, ол шабуылдардан бөлек желілік аномалияларды талдауға мүмкіндік береді. Бұл деректер жиынтығы желілік трафикті тиімді талдауға, шабуылдарды анықтауға арналған жасанды интеллект және машиналық оқыту алгоритмдерін оқытуда қолданылады [25]. Қарастырылып отырған деректер жиынтығы үшін деректерді алдын-ала өңдеу және іріктеу процедуралары егжей-тегжейлі жасалған.

Бұл модельдің басты артықшылығы-оның конволюциялық қабаттар (Conv2D) арқылы терең белгілерді алу қабілеті, бұл оны желілік шабуылдардың әртүрлі түрлерін анықтау сияқты күрделі жіктеу тапсырмаларына қолайлы етеді. Mini-VGGNet-Intrusion моделі әдеттегі Трафиктен (BENIGN) dos, DDoS, PortScan және т.б. сияқты шабуылдардың әртүрлі түрлеріне дейінгі желілік оқиғалардың 15 класын қамтитын көп класты жіктеу мәселесін шешуге

бейімделген. Mini-VGGNet — Intrusion-бұл желілік интрузияны анықтау тапсырмаларына арналған классикалық vggnet архитектурасының мамандандырылған модификациясы. 2014 жылы Симониан мен Зиссерман ұсынған түпнұсқа VGGNet кескінді жіктеу тапсырмаларына бағытталған терең және қуатты архитектурасымен танымал болды. Дегенмен, оны пайдалану көптеген қабаттар мен параметрлерге байланысты айтарлықтай есептеу ресурстарын қажет етеді. Жеңіл тапсырмалар үшін VGGNet негізгі принциптерін сақтайтын, бірақ қабаттары мен сүзгілері аз mini – VGGNet жеңілдетілген нұсқасы жасалды. Mini-VGGNet модельдің тереңдігін азайтады және аз көлемді деректерді өңдеу үшін жоғары тиімділікті сақтай отырып, оны аз ресурстарды қажет етеді.

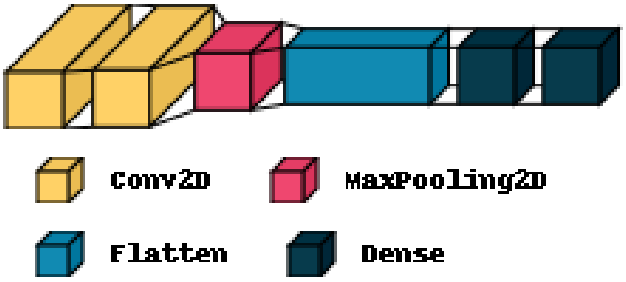
Берілген тапсырма үшін әзірленген Mini-VGGNet-Intrusion желілік деректерді талдау үшін оңтайландырылған осы архитектураны одан әрі бейімдеу болып табылады. Суреттерді өңдеу үшін сүзгілерді қолданатын түпнұсқа Mini-VGGNet-тен айырмашылығы, бұл модель \(2 \times 1\) сүзгілерін қолдана отырып, бір өлшемді немесе екі өлшемді желілік деректерге бағытталған, бұл Кеңістіктік және уақыттық белгілерді кірістерден тиімді алуға мүмкіндік береді. 2-суретте visualkeras кітапханасы арқылы бейнеленген Mini-VGGNet-Intrusion моделінің архитектурасы көрсетілген. Модельге екі конволюциялық қабат, содан кейін MaxPooling2D, сондай-ақ 15 түрлі желілік шабуыл кластарын түпкілікті жіктеу үшін екі толық байланысқан қабат кіреді (2 – сурет). Бұл архитектура DoS, DDoS және басқа да шабуылдар сияқты желілік шабуылдарды жіктеу мәселесін шешу үшін арнайы жасалған, бұл оны тиімді және ресурстары шектеулі нақты жағдайларда пайдалануды салыстырмалы түрде жеңілдетеді.



Сурет 2. Модель архитектурасы

Модель жіктеу тапсырмалары үшін деректердің кеңістіктік белгілерін түсіруге көмектесетін бірнеше конволюциялық қабаттарды қолдану арқылы жасалған. Ол деректердің өлшемін азайту және қайта оқытудың алдын алу үшін пулингті пайдаланады. Конволюция мен біріктіруден кейінгі толық байланысқан қабаттар желілік интрузияларды жіктеуге көмектеседі, белгілерді сынып ықтималдығына айналдырады. Бұл модель желілік шабуылдарды 15 түрлі сыныпқа жіктеу үшін қолданылады. Ол көп класты жіктеу үшін Adam оңтайландырғышын және sparse categorical crossentropy жоғалту мүмкіндігін пайдаланады.

3- суретте модельдің негізгі қабаттарының реттілігін көрсететін Mini-VGGNet-Intrusion архитектурасының визуализациясы көрсетілген. Архитектура деректерден негізгі белгілерді бөлетін екі конволюциялық қабаттан (Conv2D) басталады, содан кейін MaxPooling2D қабаты белгілердің Өлшемін азайтады және есептеу тиімділігін арттырады. Әрі қарай, модель екі өлшемді деректерді бір өлшемді массивке толық байланысты қабаттарға (Dense) беру үшін түрлендіретін Flatten қабатын қамтиды. Бұл қабаттар кірістерді 15 класс бойынша жіктеуге жауап береді.



Сурет 3. Модельдің негізгі қабаттары

4- суретте синтезделген нейрондық желі моделінің қабаттарының сипаттамасы келтірілген.

Model: "sequential"

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 18, 2, 32)	96
conv2d_1 (Conv2D)	(None, 17, 2, 32)	2,080
max_pooling2d (MaxPooling2D)	(None, 8, 2, 32)	0
flatten (Flatten)	(None, 512)	0
dense (Dense)	(None, 32)	16,416
dense_1 (Dense)	(None, 15)	495

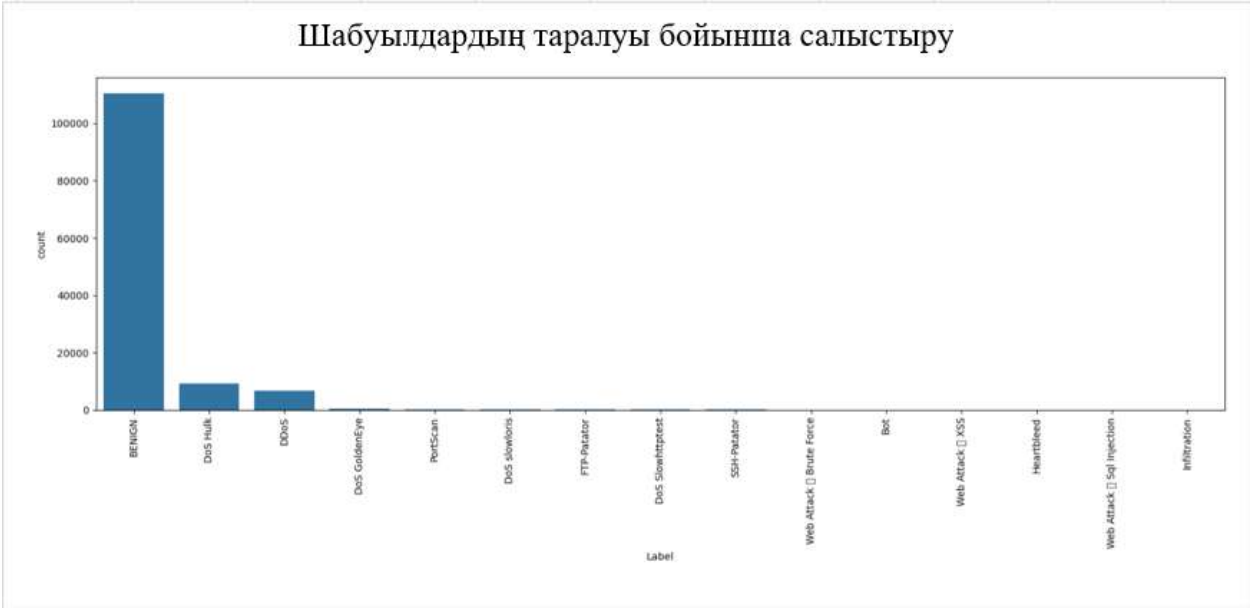
Total params: 57,263 (223.69 KB)
Trainable params: 19,087 (74.56 KB)
Non-trainable params: 0 (0.00 B)
Optimizer params: 38,176 (149.13 KB)

Сурет 4. Модельдің қысқаша сипаттамасы

Зерттеу нәтижелері

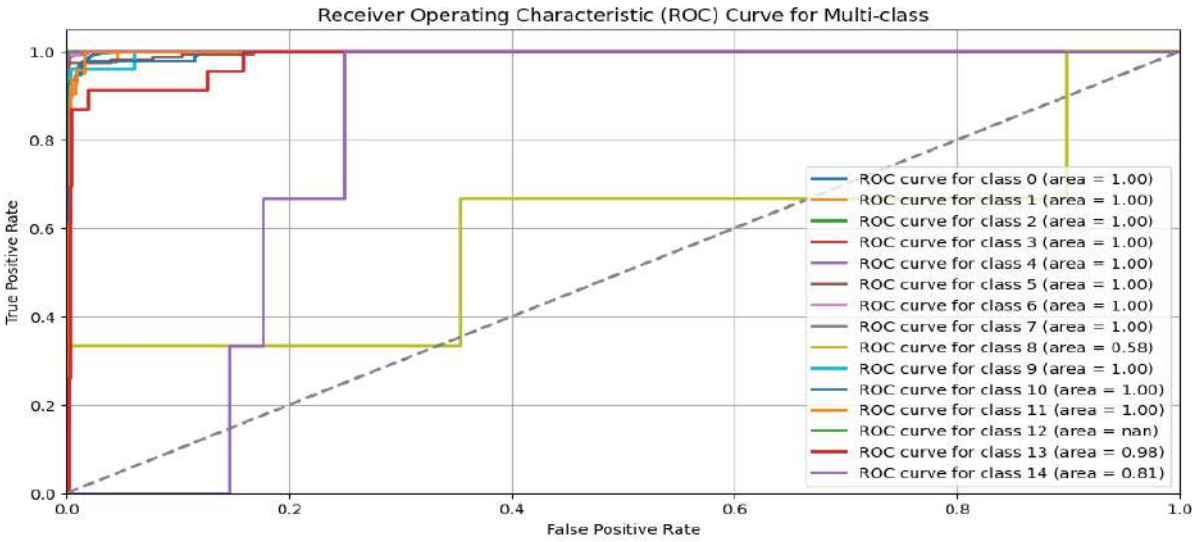
Бұл бөлімде ұсынылған модельдің архитектурасын пайдалану нәтижесінде алынған эксперименттік нәтижелерге назар аударылады.

5-суретте шабуылдардың таралуы бойынша салыстыру жүргізілді.



Сурет 5. Шабуылдардың таралуы бойынша салыстыру

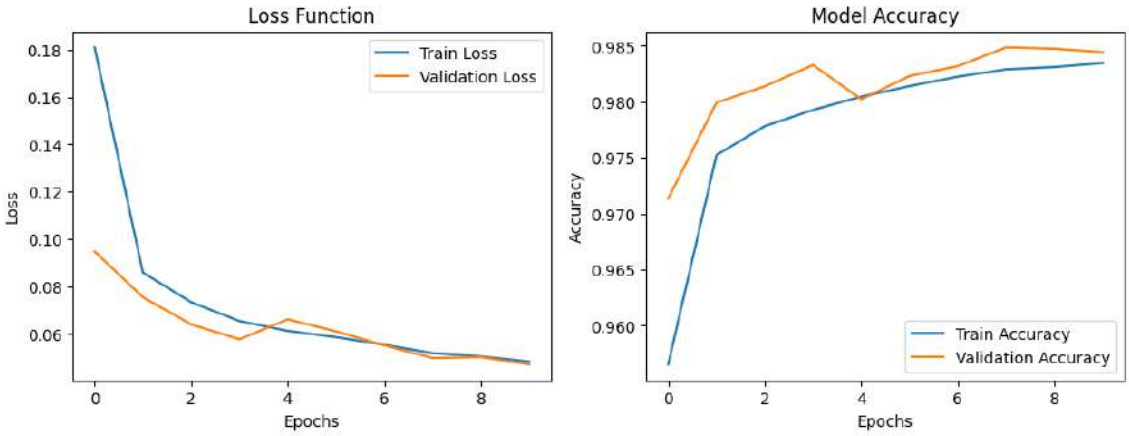
6-суретте 15 класс үшін ROC-кривалары көрсетілген, әрқайсысы түрлі классификация шектері бойынша нақты оң және жалған оң нәтижелер арасындағы байланысқа иллюстрация жасайды.



Сурет 6. Желіге рұқсатсыз енуді анықтауға арналған AUC-ROC қисығы

ROC-кривалары модельдің көпшілікті классты өте жақсы классификациялайтынын көрсетеді, мысалы, BENIGN, DoS Hulk, DDoS сияқты, мұнда AUC мәні 1.00. Алайда, Web Attack – XSS және Web Attack – SQL Injection класстары үшін AUC мәндері сәйкесінше 0.58 және 0.81 болып табылады, бұл модельдің дәлдігін жақсарту қажеттілігін білдіреді. Infiltration классы үшін AUC мәні есептелмеген, бұл деректердің жеткіліксіздігі немесе модельдің осы классты дұрыс анықтамауы мүмкін. Графиктегі сұр нүктелі сызық кездейсоқ классификацияны AUC = 0.5 ретінде көрсетеді, ал ROC-кривасы осы сызықтан неғұрлым алшақ болса, модель соғұрлым жақсы классификациялайды.

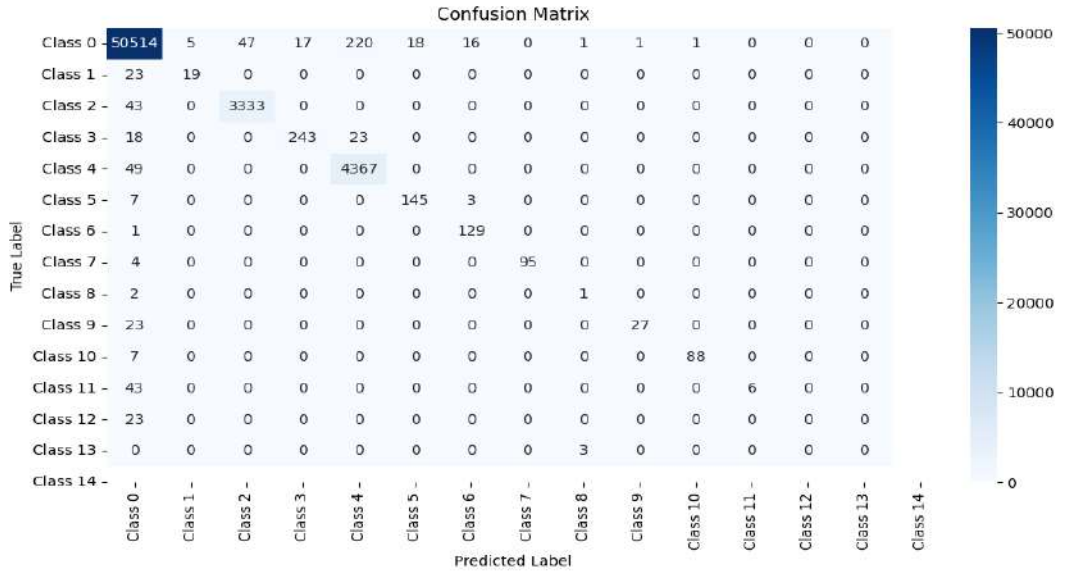
7-суретте модельдің өнімділігін және оқыту процесінің тиімділігін бағалау үшін жоғалту функциясы графигі (Loss Function) мен дәлдік графигі (Model Accuracy) пайдаланылды.



Сурет 7. Жоғалту функциясы графигі (Loss Function) және дәлдік графигі (Model Accuracy)

Жоғалту функциясы графигі: Модельдің қателігін көрсетеді. Жоғалту мәнінің төмендеуі модельдің үйреніп жатқанын және артық оқытуды анықтауға көмектеседі. Дәлдік графигі: Модельдің дұрыс болжамдарының пайызын көрсетеді. Оқыту мен валидация дәлдігін салыстыру арқылы артық оқытуды анықтауға және модельдің өнімділігін бақылауға болады. Бұл графиктер модельдің тиімділігін қадағалап, қажет болған жағдайда оның параметрлерін түзетуге мүмкіндік береді.

8-суретте қателіктерді талдауға, модель сапасының көрсеткіштерін есептеуге және сынып теңгерімсіздігін анықтауға мүмкіндік беретін конфузиялық қате матрицасы көрсетілген.



Сурет 8. Модельдің қате матрицасы

Mini-VGGNet-Intrusion дәстүрлі машиналық оқыту модельдерінен желіге рұқсатсыз енуді анықтау, деректерден күрделі белгілерді автоматты түрде алу қабілетінің арқасында артықшылыққа ие, бұл жіктеу дәлдігін жақсартады және деректерді қолмен өңдеу қажеттілігін азайтады.

2-кестеде машиналық оқыту моделдері мен ұсынылған терең оқыту моделінің алынған нәтижелерін салыстыру көрсетілген.

Кесте 2. Алынған нәтижелерді салыстыру

Қолданылған тәсілдер	*Моделдер*	*Accuracy*	*Precision*	*Recall*	*F-score*	*ROC*
Ұсынылған терең оқыту моделі	*Mini-VGGNet-Intrusion*	*0.985*	*0.988*	*0.993*	*0.987*	*0.98*
Машиналық оқыту моделдері	*NB*	*0.874*	*0.832*	*0.863*	*0.851*	*0.92*
	RF	*0.851*	*0.854*	*0.822*	*0.856*	*0.77*
	DT	*0.602*	*0.524*	*0.585*	*0.642*	*0.65*
	SVM	*0.873*	*0.852*	*0.862*	*0.851*	*0.78*
	KNN	*0.856*	*0.839*	*0.831*	*0.837*	*0.92*
	LR	*0.862*	*0.853*	*0.837*	*0.858*	*0.78*

Дискуссия

Ұсынылған модель желілік кіруді анықтау тапсырмасына бейімделген белгілі VGGNet архитектурасының модификациясы. Дегенмен, оның күрделілігі мен ресурс сыйымдылығы айтарлықтай есептеу ресурстарын қажет етеді, бұл оны ресурстары шектеулі немесе деректер көлемі аз тапсырмалар үшін әрқашан қолайлы ете бермейді. Архитектураны жеңілдету үшін MINI-VGGNet ұсынылды, ол түпнұсқа модельдің негізгі принциптерін сақтайды, бірақ қабаттар саны азаяды және желілік деректерді талдауға бейімделеді. Mini-VGGNet-Intrusion моделі Mini-VGGNet-тен ерекшеленеді, себебі ол суреттерді өңдеуге арналған стандартты сүзгілердің орнына, желілік деректерден кеңістіктік және уақыттық белгілерді тиімді түрде алуға арналған арнайы өлшемді сүзгілерді қолданады. Модель екі конволюциялық қабат, бір MaxPooling2D қабаты және екі толық байланысқан қабаттан тұрады. Бұл архитектура желілік шабуылдарды, соның ішінде DoS және DDoS сияқты 15 түрлі класты дәл анықтауға арналған. Модельдің қарапайым құрылымы мен төмен ресурстық талаптары терең желілерге қарағанда жоғары жіктеу дәлдігін сақтай отырып, есептеу ресурстарын үнемдейді. Ұсынылған модельдің желіге рұқсатсыз енуді анықтауда көптеген артықшылықтары бар, бірақ бірнеше шектеулері де бар. Біріншіден, модель уақыттық реттіліктерді тиімді меңгергенімен, оның күрделілігі мен есептеулер көп уақыт пен ресурсты талап етеді, бұл желі қауіпсіздігі үшін жылдамдық маңызды болған жағдайда қиындықтар тудыруы мүмкін. Екіншіден, ресурстары шектеулі немесе деректер көлемі аз тапсырмалар үшін әрқашан қолайлы ете бермейді.

Қорытынды

Қорытындылай келе, ұсынылған Mini-VGGNet-Intrusion моделі, әсіресе теңгерімсіз деректер жағдайында, желілік интрузияларды анықтауда айтарлықтай жетістіктер мен нәтижелер көрсетті. Оның конволюциялық қабаттарға негізделген архитектурасы шабуылдардың көптеген түрлері үшін жоғары жіктеу дәлдігін қамтамасыз етеді, бұл оны нақты интрузияны анықтау және алдын алу жүйелерінде (IDS/IPS) қолдануға мүмкіндік береді. Дегенмен, кейбір шабуылдардың жіктелуін жақсарту үшін деректердің теңгерімсіздігімен күресу әдістерін қосымша конфигурациялау және қолдану қажет. Mini-VGGNet-Intrusion классикалық VGGNet архитектурасын желілік интрузияны анықтау тапсырмасына сәтті бейімдеуді көрсетеді. Архитектураны жеңілдету және желілік деректерді оңтайландыру арқылы модель төмен есептеу шығындарын сақтай отырып, мүмкіндіктерді тиімді шығарады және дәл жіктеуді қамтамасыз етеді. Бұл оны дәстүрлі терең нейрондық желілер тым көп ресурстарды қажет ететін жағдайларда жұмыс істеуге қолайлы етеді. Осылайша, Mini-VGGNet-Intrusion дәлдік пен есептеу ресурстары арасындағы тепе-теңдікті қамтамасыз ететін желілік шабуылдарды анықтаудың тиімді шешімін ұсынады.

Пайдаланылған дереккөздер тізімі

[1] Сычев Д.И. Методы машинного и глубокого обучения для систем обнаружения вторжений: обзор и анализ // Международный журнал информационных технологий и энергоэффективности. – 2023. –Т. 8 № 4(30) с. 9–17

[2] Mohammadi S., Namadchian A. Anomaly-based Web Attack Detection: The Application of Deep Neural Network Seq2Seq With Attention Mechanism. The ISC International Journal of Information Security, vol. 12, issue 1, 2020, pp. 44-54. DOI: 10.22042/isecure.2020.199009.479.

[3] Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 // Вопросы кибербезопасности, вып. №3 (37), 2020 г., стр. 76-86. DOI: 10.21681/2311-3456-2020-03-76-86.. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain. Psychological review, vol. 65, issue 6, 1958, pp. 386-408. DOI: 10.1037/H0042519.

[4] Rumelhart D.E., Hinton G.E., Williams R.J. Learning Internal Representations by Error Propagation. In: Rumelhart, D.E. and McClelland, J.L., The PDP Group, Eds., Parallel Distributed Processing: Explorations in the Microstructure of Cognition, Volume 1, Foundations, MIT Press, Cambridge, 1985, pp. 318-362.

[5] Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. Available at: http://www.deeplearningbook.org.

[6] Culurciello E. The fall of RNN / LSTM (2018). Available at: https://towardsdatascience.com/the-fall-ofrnn-lstm-2d1594c74ce0.

[7] Google Scholar. Available at: https://scholar.google.com, accessed 04.10.2023.

[8] Harzing A.W. Publish or Perish (2007). Available at: https://harzing.com/resources/publish-or-perish.

[9] Jiang K., Wang W., Wang A., Wu H. Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network. IEEE Access, vol. 8, 2020, pp. 32464-32476. DOI: 10.1109/ACCESS.2020.2973730.

[10] Vigneswaran R.K., Vinayakumar R., Soman K.P., Poornachandran P. Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-6. DOI: 10.1109/ICCCNT.2018.8494096.

[11] Khan M.A. HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System. Processes, vol. 9, issue 5: 834, 2021, 14 p. DOI: 10.3390/pr9050834.

[12] Xiao Y., Xing C., Zhang T., Zhao Z. An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access, vol. 7, 2019, pp. 42210-42219. DOI: 10.1109/ACCESS.2019.2904620.

[13] Li Z., Qin Z., Huang K., Yang X., Ye S. Intrusion Detection Using Convolutional Neural Networks for Representation Learning. In: Liu D., Xie S., Li Y., Zhao D., El-Alfy ES. (eds) Neural Information Processing. ICONIP 2017. Lecture Notes in Computer Science, vol. 10638. Springer, Cham, 2017, pp. 858-866. DOI: 10.1007/978-3-319-70139-4_87.

[14] Yin C., Zhu Y., Fei J., He X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, vol. 5, 2017, pp. 21954-21961. DOI: 10.1109/ACCESS.2017.2762418.

[15] Sheikhan M., Jadidi Z., Farrokhi A. Intrusion detection using reduced-size RNN based on feature grouping. Neural Computing and Applications - NCA, vol. 21, no. 6, 2012, pp. 1185–1190. DOI: 10.1007/s00521-010-0487-0.

[16] . Sumaiya Thaseen I., Saira Banu J., Lavanya K., Rukunuddin Ghalib M., Abhishek K. An integrated intrusion detection system using correlation-based attribute selection and artificial neural network. Transactions on Emerging Telecommunications Technologies, vol. 32, issue 2: e4014, 2021, 15 p. DOI: 10.1002/ett.4014.

[17] Ramaiah M., Chandrasekaran V., Ravi V., Kumar N. An intrusion detection system using optimized deep neural network architecture. Transactions on Emerging Telecommunications Technologies, vol. 32, issue 4: e4221, 2021, 17 p. DOI: 10.1002/ett.4221.

[18] Xu C., Shen J., Du X., Zhang F. An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units. IEEE Access, vol. 6, 2018, pp. 48697-48707. DOI: 10.1109/ACCESS.2018.2867564.

[19] Le T.-T.-H., Kim Y., Kim H. Network Intrusion Detection Based on Novel Feature Selection Model and Various Recurrent Neural Networks. Applied Sciences, vol. 9, no. 7: 1392, 2019, 29 p. DOI: 10.3390/app9071392.

[20] Drewek-Ossowicka A., Pietrołaj M., Rumiński J. A survey of neural networks usage for intrusion detection systems. Journal of Ambient Intelligence and Humanized Computing, vol. 12, 2021, pp. 497–514. DOI: 10.1007/s12652-020-02014-x.

[21] Liu H., Lang B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences, vol. 9, no. 20: 4396, 2019, 28 p. DOI: 10.3390/app9204396.

[22] Getman A.I., Goryunov M.N., Matskevich A.G., Rybolovlev D.A., Nikolskaya A.G. Deep Learning Applications for Intrusion Detection in Network Traffic. Trudy ISP RAN/Proc. ISP RAS, vol. 35, issue 4, 2023. pp. 65-92.

[23] Intrusion Detection Evaluation Dataset (CICIDS2017). Available at: https://www.unb.ca/cic/datasets/ids2017.html, accessed 16.08.2020

References

[1] Sychev D.I. Metody mashinnogo i glubokogo obucheniya dlya sistem obnaruzheniya vtorzheniy: obzor i analiz // Mezhdunarodnyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti. – 2023. – T. 8 № 4(30). – S. 9–17.

[2] Mohammadi S., Namadchian A. Anomaly-based Web Attack Detection: The Application of Deep Neural Network Seq2Seq With Attention Mechanism. The ISC International Journal of Information Security, vol. 12, issue 1, 2020, pp. 44-54. DOI: 10.22042/isecure.2020.199009.479.

[3] Gayfulina D.A., Kotenko I.V. Primenenie metodov glubokogo obucheniya v zadachakh kiberbezopasnosti. Chast' 1 // Voprosy kiberbezopasnosti. – 2020. – Vyp. №3 (37). – S. 76-86. DOI: 10.21681/2311-3456-2020-03-76-86.

[4] Rumelhart D.E., Hinton G.E., Williams R.J. Learning Internal Representations by Error Propagation. In: Rumelhart, D.E. and McClelland, J.L., The PDP Group, Eds., Parallel Distributed Processing: Explorations in the Microstructure of Cognition, Volume 1, Foundations, MIT Press, Cambridge, 1985, pp. 318-362.

[5] Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. Available at: http://www.deeplearningbook.org.

[6] Culurciello E. The fall of RNN / LSTM (2018). Available at: https://towardsdatascience.com/the-fall-ofrnn-lstm-2d1594c74ce0.

[7] Google Scholar. Available at: https://scholar.google.com, accessed 04.10.2023.

[8] Harzing A.W. Publish or Perish (2007). Available at: https://harzing.com/resources/publish-or-perish.

[9] Jiang K., Wang W., Wang A., Wu H. Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network. IEEE Access, vol. 8, 2020, pp. 32464-32476. DOI: 10.1109/ACCESS.2020.2973730.

[10] Vigneswaran R.K., Vinayakumar R., Soman K.P., Poornachandran P. Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-6. DOI: 10.1109/ICCCNT.2018.8494096.

[11] Khan M.A. HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System. Processes, vol. 9, issue 5: 834, 2021, 14 p. DOI: 10.3390/pr9050834.

[12] Xiao Y., Xing C., Zhang T., Zhao Z. An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. IEEE Access, vol. 7, 2019, pp. 42210-42219. DOI: 10.1109/ACCESS.2019.2904620.

[13] Li Z., Qin Z., Huang K., Yang X., Ye S. Intrusion Detection Using Convolutional Neural Networks for Representation Learning. In: Liu D., Xie S., Li Y., Zhao D., El-Alfy ES. (eds) Neural Information Processing. ICONIP 2017. Lecture Notes in Computer Science, vol. 10638. Springer, Cham, 2017, pp. 858-866. DOI: 10.1007/978-3-319-70139-4_87.

[14] Yin C., Zhu Y., Fei J., He X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, vol. 5, 2017, pp. 21954-21961. DOI: 10.1109/ACCESS.2017.2762418.

[15] Sheikhan M., Jadidi Z., Farrokhi A. Intrusion detection using reduced-size RNN based on feature grouping. Neural Computing and Applications - NCA, vol. 21, no. 6, 2012, pp. 1185–1190. DOI: 10.1007/s00521-010-0487-0.

[16] . Sumaiya Thaseen I., Saira Banu J., Lavanya K., Rukunuddin Ghalib M., Abhishek K. An integrated intrusion detection system using correlation-based attribute selection and artificial neural network. Transactions on Emerging Telecommunications Technologies, vol. 32, issue 2: e4014, 2021, 15 p. DOI: 10.1002/ett.4014.

[17] Ramaiah M., Chandrasekaran V., Ravi V., Kumar N. An intrusion detection system using optimized deep neural network architecture. Transactions on Emerging Telecommunications Technologies, vol. 32, issue 4: e4221, 2021, 17 p. DOI: 10.1002/ett.4221.

[18] Xu C., Shen J., Du X., Zhang F. An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units. IEEE Access, vol. 6, 2018, pp. 48697-48707. DOI: 10.1109/ACCESS.2018.2867564.

[19] Le T.-T.-H., Kim Y., Kim H. Network Intrusion Detection Based on Novel Feature Selection Model and Various Recurrent Neural Networks. Applied Sciences, vol. 9, no. 7: 1392, 2019, 29 p. DOI: 10.3390/app9071392.

[20] Drewek-Ossowicka A., Pietrołaj M., Rumiński J. A survey of neural networks usage for intrusion detection systems. Journal of Ambient Intelligence and Humanized Computing, vol. 12, 2021, pp. 497–514. DOI: 10.1007/s12652-020-02014-x.

[21] Liu H., Lang B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences, vol. 9, no. 20: 4396, 2019, 28 p. DOI: 10.3390/app9204396.

[22] Getman A.I., Goryunov M.N., Matskevich A.G., Rybolovlev D.A., Nikolskaya A.G. Deep Learning Applications for Intrusion Detection in Network Traffic. Trudy ISP RAN/Proc. ISP RAS, vol. 35, issue 4, 2023. pp. 65-92.

[23] Intrusion Detection Evaluation Dataset (CICIDS2017). Available at: https://www.unb.ca/cic/datasets/ids2017.html, accessed 16.08.2020