School of Information Technology & Engineering

WINTER SEMESTER 2021-2022

SWE 3002: Information System Security

Digital Assignment-1

Name : S.Deepan

Regno : 19MIS0102

Slot : E2+TE2

Topic: Assessment on applicability and adoptability of AI and ML techniques to improve Information Systems security in the domain of "Anomalous behavior detection".

Faculty:

Dr. M. Sudha

Associate Professor, SITE

Team Details:

Names	Year
19MIS0048 SHATAKSHI JHA 19MIS0056 V DANUSHRAM 19MIS0061 SHREE HARAN S	2017
19MIS0069 SIRAJUDEEN P 19MIS0092 LATHA SHREE R 19MIS0099 B THULASI	2018
19MIS0102 S DEEPAN 19MIS0105 ADDIKAM SAI PRANAV 19MIS0114 KUMMARA PRATHYUSHA 19MIS0117 BIRRU JHANSI DURGA DEVI	2019
19MIS0131 PRADNESH A 19MIS0140 M YUGANDHAR 19MIS0143 DESIREDDY NIRANJAN REDDY	2020,2021

Year	Article Information	Literature Review
2017	**Multi-Perspective Machine**	**KEY WORDS:**

	Learning a Classifier Ensemble Method for Intrusion Detection **AUTHORS:** Sean T Miller **CITATION:** https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&as_vis=1&q=2017+research+paper+on+artificial+intelligence+and+machine+learning+to+improve+information+security+Sean+t+miller&btnG=#d=gs_qabs&u=%23p%3Dp7M7NxHMeF4J	● Machine learning; ● ensemble methods; ● Cybersecurity; ● Anomalous detection. **SHORT DESCRIPTION:** In today's society, cyber security is one of the most significant and dynamic fields. There are various detection mechanisms for each given cyber-attack. Every detection technique is based on one or more network properties. **PROBLEM SOLUTION:** The primary principle underlying MPML is that by combining features that support the same qualities into feature subsets called perspectives, we may encourage variety across views (classifiers in the ensemble) and enhance prediction accuracy. **APPLICATIONS:** Multiview learning, ensemble approaches, and multiperspective machine learning are some of the key studies in this topic. In this study, a machine learning ensemble approach to multi-perspective machine learning is investigated (MPML) **IMPLEMENTATION FRAMEWORK:** The purpose of multi-perspective machine learning (MPML) is to improve the accuracy of malware detection via the use of carefully selected malware characteristics. These characteristics are displayed in the form of a variety of indicators. **CONCLUSION AND RESULTS:** Initial effects at the NSL- KDD dataset display at least a 4% development over different ensemble strategies together with bagging boosting rotation woodland and random for- est. The intention may be to automate the angle

		advent process. Different ML algorithms might also additionally have exceptional results on exceptional angles. Optimizing overall performance via an angle set of rules mixture can also be explored in paintings to come.
2017	**Machine Learning and Images for Malware Detection and Classification** **AUTHORS:** Konstantinos Kosmidis **CITATION:** https://www.researchgate.net/publication/321345158_Machine_Learning_and_Images_for_Malware_Detection_and_Classification	**KEYWORDS:** ● Malware analysis ● malware detection ● machine learning ● computer vision ● image processing, classification ● clustering **SMALL DESCRIPTION:** Detecting malicious code with genuine suits on gathered datasets is turning into a large-scale identity hassle because of the lifestyles of latest malware variants. Being capable of directly and correctly picking out new assaults permits protection specialists to reply effectively. **IMPLEMENTATION FRAMEWORK:** 1. Procedures and steps taken for the education of the version is cited below: 2. Set information matrix with capabilities as initiator and activator. 3. The scale of the access tier is identical to the matrix size. 4. Insert and Put preliminary values to the primary hidden tier. 5. Calculate effects of the hidden tier with using the weights and the initiation services. 6. Allow and set consequences extra later till you compute the very last tier. **APPLICATIONS:** ● PERCEPTRON ● MULTILAYER PERCEPTRON

		● RANDOM FOREST ● NEAREST CENTROID **OUTCOMES AND GOALS:** To broaden an automatic framework for identity of unknown vulnerabilities via means of leveraging present day neural community techniques. This has a big and instantaneous price for the safety field, as present day anti-virus software programs are generally capable of apprehending the most effective after its infection, and preventive measures are limited. **CONCLUSION:** The fee of automatic identity is really fairly vital on the grounds that function engineering is each a time-eating and time-touchy task. with new malware studied even as being located withinside the wild. For the future, there's a want to enhance the algorithms advised or recommend new ones.
2017	**An Empirical Evaluation for The Intrusion Detection Features Based on Machine Learning and Feature Selection Methods** **AUTHORS:** MOUHAMMD ALKASASSBEH Computer Science Department, Information Technology College, Mutah University, Jordan **CITATION:** https://arxiv.org/abs/1712.09623	In the present world of great advances in the fields of Artificial Intelligence and machine learning, with the advances also came the development of penetration and intrusion. This causes a great risk to the organisations, government agencies, and might cause large economic losses. To prevent this there are many techniques designed for protection like firewall and IDS (intrusion detection systems). IDS is nothing but a set of software and hardware used to detect hacker activities which are an anomalous. IDS uses two types of anomalies to detect to detect hacker activities which are different from a normal user's activities. The significance of IDS is to identify anomalous activities and unauthorized access

		attempting to breach the confidentiality, integrity of the organisation or government or an individual. This paper analyses and studies the intrusion detection problem using three machine learning algorithms mainly and they are: • BayesNet Algorithm • Multi-Layer Perceptron (MLP) • Support Vector Machine (SVM) These algorithms are applied on real life, and Management Information Based dataset (MIB) is collected from the inputs of the real-world data, and further to enhance the increase the accuracy of the detection process, a set of feature selection approaches are used and they are: • Infogain (IG) • ReliefF (RF) • Genetic Research (GS) With the experiments done for the research it shows that the feature selection methods have increased the accuracy and mainly the BayesNet with the GS gives 99.9% accuracy rate.
2017	**A Study on Intrusion Detection Using Centroid-Based Classification** **AUTHORS:** Bambang Setiawan*,	The goal of the intrusion detection system (IDS) is to achieve the highest possible accuracy to detect possible attacks and intrusions. The IDS system has many fallbacks and weaknesses, mainly when they fail to detect and recognize new attacks

	Supeno Djanali, Tohari Ahmad Department of Informatics, Institut Teknologi Sepuluh Nopember, Sukolilo, Surabaya, 16011, Indonesia **CITATION:** https://www.sciencedirect.com/science/article/pii/S1877050917329721	because the signatures are unknown. And also, a new system behaviour which might be a normal one but not stored in database will be recognized as an anomaly and will be marked as an intrusion or hack. So, because of this problem, there is a potential system failure when the IDS are disabled and it will provide an opportunity for the hackers and intruders to compromise the system and they will infiltrate the organisations' network and their systems. To solve this the research paper studies the use of Centroid-Based Classification for Intrusion Detection. This paper studies 60 papers which were associated in the period between 2010 to 2016 focusing on developing an intrusion detection system (IDS) using hybrid classifiers. Out of these 60 papers in which 11 papers study about Centroid-Based classification. So the accomplishments and limitations in developing IDSs using hybrid machine learning is discussed and how Centroid-Based classification can improve the anomalous behaviour detection is studies deeply in this paper.
2017	**"Machine learning to detect anomaliesin web log analysis," 2017 3rd IEEE In-ternational Conference on Computer and Communications (ICCC), 2017, pp.519-523, doi: 10.1109/ CompComm.2017.8322600.** **AUTHORS:** Cao, Y. Qiao and Z. Lyu,	In this article, the authors Qimin Cao, Yinrong Qiao has discussed about the Machine Learningto Detect Anomalies in Web Log Analysis. They have mentioned that because of their greatvalue, Web servers are easily attacked as in- formation technology grows rapidly. As a result, web security has attracted the interest of both academia and industry. Anomaly detection is vi-tal in the field of Web security, and log mes- sages containing extensive system runtime in- formation have become an

	CITATION: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8322600&isnumber=8322494	important data ana- lysis object as a result. This paper says that the traditional log anomaly detection relies on pro- grammers manually inspecting logs using keyword searches and regular expression matches. Although programmers can apply in- trusion detection systems to decrease their bur-den, the log system data is vast, attack types vary, and hacking capabilities increase, making traditional detection ineffective. Many anomaly detection processes, particularly the machine learning method, have been proposed in recent years to improve traditional detection techno- logy. In this research, a two-level machine learning technique is used to propose an anomaly detection system for web log files. The decision tree model organizes data sets into normal and abnormal categories. The construction of mul- tiple HMMs in the usual data set is manually checked and the experimental data comes from a real-world industrial setting, where log files were collected and several true intrusion notifications were found. The experimental results on this data set reveal that this system achieves higher detection accuracy and can discover un- known anomaly data when compared to three types of machine learning algorithms utilized in anomaly detection.
2017	**"Machine Learning for Anomaly Detec-tion and Categorization in Multi-CloudEnvironments," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 97-103, doi: 10.1109/CSCloud.2017.15.** **AUTHORS:**	T. Salman, D. Bhamare, A. Erbad, R. Jain and M. Samaka have addressed the cloud computing has been widely utilized by application service providers and businesses to decrease both cap- ital and operational expenditures. Previously private data center applications and services arenow being transferred to private or public clouds. They mentioned that in multi-cloud environments, firewalls and typical rule-based

	T. Salman, D. Bhamare, A. Erbad, R. Jain and M. Samaka, **CITATION:** https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7987183&isnumber=7987154	se- curity protection techniques are insufficient to secure user data. Advances in machine learning techniques have recently ignited researchers' in-terest in developing intrusion detection systems (IDS) that can detect anomalies in network data.The majority of research, on the other hand, does not distinguish between different sorts of attacks. In this paper they examine into both identifying and categorizing anomalies, rather than only detecting, as is the norm in most re- cent research. They built and tested learning models for both detection and categorization ofdistinct assaults using a large publicly available data set. Also they employed two supervised machine learning algorithms, namely linear re- gression (LR) and random forest, to be exact (RF). He concluded that supervised machine learning approaches can be used to detect anomalies and characterize attacks. The UNSWdata set was chosen since it is the most recent and complete data set widely available. The res-ults show that the random forest (RF) technique,along with a feature selection scheme, can de- tect anomalies with 99 percent accuracy.
2018	**Author = {Lee, Sangdo and Shin, Yongtae},** **year = {2018},** **month = {01},** **title = {The Direction of Information Security Control Analysis Using Artificial Intelligence},** **isbn = {978-981-10-7604-6},** **doi = {10.1007/978-981-10-7605-3_138}**	The paper provides information about artficial intelligence utilization which is expanding slowly in the modern. it explains about the codes in the security region and it states that minimum 200,000 security breaches are occuring daily and regularly it burning through a lot of their time in following incorrectly targets or assaulting techniques. In this review, we have concentrated on the chance of using current AIs utilized for determination of tumors, interpretations or straightforward discussions, alongside the future heading of

	CITATION: https://www.researchgate.net/publication/321948157_The_Direction_of_Information_Security_Control_Analysis_Using_Artificial_Intelligence	AI for security control. The concentrate likewise endeavors to observe a viable strategy for diminishing harms by quickly investigating assault techniques and weaknesses, trusting the technique will be powerful in safeguarding the frameworks from another assortment of assaults.
2018	**Author={Haripriya, L. and Jabbar, M.A.},** **Booktitle={2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)},** **Title={Role of Machine Learning in Intrusion Detection System: Review},** **Year={2018},** **Pages={925-929},** **Doi=10.1109/ICECA.2018.8474576** **CITATION:** https://ieeexplore.ieee.org/document/8474576/citations#citations	In this paper, they discussed various Machine Learning (ML) Techniques for detection of Intrusion Detection System (IDS). Also in this paper they discussed about the detail about comparison of various approaches for Intrusion Detection System (IDS) using ML is given. Each algorithm has its own importance in the improvement of IDS when compared to other algorithms. It is very difficult to train the lgorithms when certain amount of traffic data is not available. This is the limitation which has to be improved. Hence we cannot select a particular technique for implementing IDS. Therefore improvements have to be done to the ML techniques that will be helpful in reducing the false alarm rate and increasing detection rate.
2018	**Towards Intelligent Intrusion Detection Systems for Cloud Computing by Mohammed J Aljebreen, 2018.** **CITATION:** https://repository.lib.fit.edu/bitstream/handle/11141/255	**In this research paper,** an intrusion detection system was developed for containers running in the cloud environment. One of the main characteristics of a cloud-based intrusion detection system is that it works in real-time and detects a variety of attacks with minimal False Positive Rates. The following objectives have been

	4/ALJEBREEN-DISSERTATION-2018.pdf?sequence=1&isAllowed=y	implemented in this paper: • Developing an intrusion detection system for containers running in the cloud environment. • Designing and implementing a cloud environment that was used to collect real world data that was used for testing the proposed intrusion detection system. • Developing a data representation mechanism that allows the intrusion detection systems classifiers to learn the model quickly and accurately. • Designing and developing an intrusion detection system framework for both anomaly and misuse detection techniques. • Applying and implementing sophisticated machine learning algorithms and evaluating their performance and detection abilities. **The developed cloud-based intrusion detection system** has the following characteristics • Reliability • Quality of Service (QoS) • Agility and adaptability • Availability **In anomaly intrusion detection,** it is assumed that the nature of the intrusion is unknown, but that the intrusion will result in behavior different from that normally seen in the system. In this research, he **proposed intrusion detection system** is a **host-based system.** **In this research, the sliding window**

		technique was used, along with other factors to enrich the **representation of the data** in order to design efficient, fast, simple, and intelligent intrusion detection systems that give better results for containers in cloud environments. **The Environment Design** In order to test the proposed intrusion detection systems realistically, real world data has to be used.This research's cloud environment used the O**penStack deployment.** For **the anomaly detection,** two algorithms were used to detect anomalies: the Interquartile range (IQR) and a K-nearest Neighbor that uses a euclidean distance-based metric. For the misuse detection, several machine learning algorithms were used to detect anomalies as follows: Artificial Neural Networks (ANNs), C4.5 decision tree, Random Forests, and Support Vector Machines (SVM) **In Conclusion,** after building the cloud environment, the MySQL container was used to gather the data during the running time in the cloud.The results show that using the machine learning techniques give more accurate detection and maintain high true positive rates and low false positive rates, where some algorithms, such as SVM and RF, achieved a 100% 108 detection rate with a 0.00% false positive rate.
2018	**Protecting Cyber Physical Production Systems using Anomaly Detection to enable Self-adaptation**	Cyber Physical Production Systems (CPPS) will turn into the foundation of the current industry. Safeguarding them against complex cyber threats is a fundamentally important worry for the future execution of

	AUTHORS: Giuseppe Settanni, Florian Skopik, Anjeza Karaj, Markus Wurzenberger, Roman Fiedler Center for Digital Safety and Security AIT Austrian Institute of Technology - Vienna, Austria **firstname.lastname@ait.ac.at** 2018 **CITATION:** G. Settanni, F. Skopik, A. Karaj, M. Wurzenberger and R. Fiedler, "Protecting cyber physical production systems using anomaly detection to enable self-adaptation," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), 2018, pp. 173-180, doi: 10.1109/ICPHYS.2018.8387655.	Industry 4.0, as various difficulties connected with data protection, safety, and security, become critical in this domain. A broad range of vulnerabilities can expose industrial endpoints to security threats in areas spanning from change and configuration management, software development, and access control management. The threats occur on many layers, for example, the sensor and actuator layer is usually targeted by brute force attacks, dictionary attacks, and power consumption attacks, and on the Information layer eavesdropping and traffic analysis can be put in place to acquire sensitive data from the system. Therefore a comprehensive approach is required to protect such an infrastructure, which takes advantage of the distributed nature of CPPS, and leverages the integrated IT technologies not only to increase productivity, but also to enhance security. Self-adaptive CPPS flexibly and timely configure themselves and swiftly adjust to adverse and suboptimal conditions, guaranteeing the system to always operate above a predefined performance level. This paper tells us how to detect critical threats, and, based on a series of defined security metrics, it permits to instantiate the self-adaption process, hence containing the detected attack, and mitigating its impact on the CPPS. The paper proposes the adoption of this reference model as a suitable approach to facilitate self-adaptation in CPPS, and had illustrated how anomaly detection methods facilitate the phases of monitoring and analysis of this cycle.

		MAPE-k Cycle Cyber-physical systems (CPPS) seamlessly integrate computational and physical components. Adaptability, realized through feedback loops, is a key requirement to deal with uncertain operating conditions in CPPS. Among the existing models, the MAPE-K feedback loop is the most influential reference control model for autonomic and self-adaptive systems. CPPS can benefit from the adoption of anomaly detection techniques to facilitate self-protection. The introduction of the concept of anomaly detection as enabler of the monitoring and analysis phases in the MAPE-k control loop has been done in the paper. Finally, the demonstration, through an illustrative example implemented in a laboratory testbed that how anomaly detection methods (e.g., ÆCID) can allow a CPPS to timely reveal and react to a complex cyber threat.
2018	**Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study** **AUTHORS:** Davy Preuveneers, Vera Rimmer, Illias Tsingenopolous, Jan Spooren, Wouter Joosen, Elisabeth llie- Zudor **CITATION:** Applied Sciences | Free Full-Text | Chained Anomaly	The adoption of system learning and deep learning is at the upward thrust inside the cybersecurity domain wherein these AI strategies assist beef up traditional gadget monitoring and danger detection solutions. To cope with the increasing time-to-detection of these stealthy attacks, interconnected and federated getting to know systems can enhance the detection of malicious conduct by becoming a member of forces and pooling together tracking statistics. We describe a permissioned blockchain-based totally federated learning technique where incremental updates to an anomaly detection device mastering model are chained collectively on the distributed ledger. Experiments with a sensible intrusion detection use case and an

	Detection Models for Federated Learning: An Intrusion Detection Case Study (mdpi.com)	autoencoder for anomaly detection illustrate that the improved complexity because of blockchain generation has a limited performance impact at the federated getting to know, varying between 5 and 15%, even as presenting full transparency over the disbursed education manner of the neural community. gadget gaining knowledge of (ML)-primarily based anomaly detection requires enough quantities of data to set up a baseline of regular behavior, expected noise, and bizarre deviations. In complex environments where a couple of entities should be monitored for anomalies, centralizing all statistics for schooling and testing purposes may not be viable because of aid constraints, security and privacy worries, or unacceptable communication latencies to switch the raw information . furnished an intensive review of intrusion detection and intrusion reaction structures. They provided a taxonomy of various layout parameters and classify present schemes.
2018	**Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review** **AUTHORS:** Zhiyuan Chen, Le Din Van Khoa, Ee Na Teoh, Amril Nazir, Ettikan Kandasamy Karuppiah, Kim Sim Lam **CITATION:** Machine learning	Cash laundering has been affecting the global financial system for decades. massive sums of money are laundered every year, posing a threat to the global economic system and its security.money laundering encompasses unlawful sports which might be used to make illegally received budget seem prison and valid. This paper objectives to offer a comprehensive survey of machine mastering algorithms and methods implemented to detect suspicious transactions. specially,answers of anti-money laundering typologies, link analysis, behavioural modelling, threat scoring, anomaly detection, and geographic functionality had been recognized and

	techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review | SpringerLink	analysed It should be referred to that present day business AML solution device consists of multiple detection equipment to perceive suspicious transactions [26]. seeing that wonderful processes have been applied for AML cases, this paper will not try and cover all of them. dialogue of these AML answers for this take a look at is focused on six commonplace elements, which might be AML typologies, link evaluation, move-channel guide geographic functionality, behavioural modelling, danger scoring, and anomaly detection. these factors are generated from the understand your consumer tenet (KYC) which is a preferred method for monetary institution towards AML
2019	**Hybrid Deep Learning-based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective.** **AUTHORS:** Sahil Garg, Member, IEEE, Kuljeet Kaur, Member, IEEE, Neeraj Kumar, Senior Member, IEEE, and Joel J. P. C. Rodrigues, Senior Member, IEEE **Citation:** Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia	Now-a-days social media became a part in the human life. Without social media there is no life in this technical world. So with the use of multimedia based applications grown to the top of the market. As we know that social media applications are increasing day by data and the users are registering into it. So the users will be experted to have proper multimedia network like scalability, reliability and quality of information and also service many more. So it should be a trust-based bonding between the product and the user. So the users data should be maintained securely there are several factors in the market like run-time security and energy wave control to main the secure data but Software defined network plays a major role to enhance the reliability of hybrid deep learning based anomaly detection to protect the social media content. This paper provides an investigation about the analysis of anomalous behaviour related with social

	perspective	media and it is solved by the deep learning (SDN) **Implementation Framework:** 1. Two different case studies were discussed in this paper and also achieved an accuracy of 98%. 2. Working methodology of the proposed scheme 3. Dimensionality Reduction using RBM 4. To perform the study and perform those algorithm done by using the Matlab on the Intel of 8GB RAM by using deep learning. 5. Two dataset were considered real time dataset and bench mark dataset. The real time dataset had taken from Thapar Institute of Engineering and Technology in patiala, India. The bench mark dataset has evaluated for the proposed models over five million records. 6. Two different algorithm were used in this project the first one is suspicious flow detection in the application and the second one is working methodology of the proposed scheme and other one is dimensionally reduction using RBM. To detect the accuracy following formula is used $P(h, v; \theta) =1z(\theta)exp(aTh+bTv+vTWh)$ W = Weight of packet a and b are bias value Z = partitioning function h = no of hidden units v = visible units. 7. First case study : It refers to the real-time-data-set which point out the anomalous

		behaviour in the social media dataset. The result shown is real time data set has high performance over the existing schemes. 8. Second case study : Relatively 98 to 99% of accuracy is provided on the inserted dataset **Applications:** 1. It focusses on the end to end user application 2. So these application are controlled by the software defined networking controller. 3. The project has been evaluated with the performance of the designed module on the real-time data set and the bench mark data set by using deep learning. 4. This project protect the data from the anomalous behaviour detect. **Working of SDN using deep learning (ML):** Consider a data plan where the user use more than a single application if suppose person 1 on instagram requested initiated to the database and person 2 can request on different application to the database and these data are created a flow table and send the data to the SDN control plane where it is going to check the anomalous detection of data then the report. is generated and the report is forward. to the user so these process occurs in the format of flow routing. **Functionality :** • SDN basically controls all the switches, routes, gateway and many more in the network device program. • After completing the project the SDN provides to the system with dynamic and scalable architecture to the

		application from the physical network topology. • SDN provides the runtime security, privacy to the user data without attacking from the anomalous detection of data. **Conclusion:** As per the recent insights four billion people are connect to the internet and out of that more over three billion people are registered in the social media platform so the network become more vulnerable to the security risk in the platform like Whatsapp, Skipe etc. Hence the data should be secure in real time so software defined network are designed to detect the real time data anomaly detection in those application.
2019	**Anomaly Detection in Smart Environments using Artificial Intelligence**. **AUTHORS:** Diego Moreira, Humberto Marques, Joaquim Celestino Jr. and Rafael L. Gomes Aldri Santos and Michele Nogueira **Citation:** DEA: Anomaly Detection in Smart Environments using Artificial Intelligence.	Technology are improving a lot and the society is turning into the smart environment. The smart environment contains smart house, smart city with IOT devices where we can communicate with the device which is connected to the internet. If those IOT devices subject to the anomalous behaviour it is due to the malfunction. Checking those problems in the IOT devices will be a huge task to the user. To resolve these problem in this paper they subjected to Digital Encryption Algorithm project refers to the system based Artificial intelligence which checks or monitor the error in malfunctions or the security problem and finally detects the anomalous behaviour of the devices in this smart environment. So these artificial intelligence plays a major role to find the problem of the device and respond quickly. **Implementation Framework:**

		The smart environment consists IOT devices like sensor, smart house and technical stuffs. Each devices have there own functionalities. If there is any defect like malfunction occurs it will be rectified with AI technique and Azure platform. The azure platform allows the deployment of machine learning solution to generate the solution and upgrade it automatically. **Working Process :** This project contains sequential dataset which was fetched from the Federal university given as input to the system which contains the network services like Telnet, data volume in a connection. Then the result is evaluated with the AI technique like Random forest which generates the accuracy of 79.41%, K-nearest neighbour with the accuracy of 79.51%, RNN and the decision tree with the accuracy of 80.58%, 82.71%. Hence by seeing the accuracy we can conclude that AI technique can detect the anomalous detection in lot of IOT devices. **Applications :** 1. The digital encryption algorithm project behaviour like a profile which contains a pack of source and designation address and active flow. So it points out the anomalous behaviour. 2. The initial experiment conducted on the basis of NSL-KDD databases which also contain the packets,flows and devices. 3. To perform the above activity nine IOT devices with varies functionality were connected to solve the problem of

		botnet detection in IOT. **Conclusion:** Smart environment contains a lot of IOT devices which are connected to the internet can be subjected to anomalous behaviour which results to malfunction to rectify this type of problems the DEA project can monitor those problems with the help of artificial intelligence technique.
2019	**Spatiotemporal Anomaly Detection using Deep Learning for Real-time Video Surveillance** **AUTHORS:** Rashmika Nawaratne, Damminda Alahakoon, Member, IEEE, Daswin De Silva, Member, IEEE, and Xinghuo Yu, Fellow, IEEE **CITATION:** https://ieeexplore.ieee.org/abstract/document/8820090	In the rapid developments in autonomous industrial environment , the need of intelligent real time video surveillance is must and should . Recent developments in artificial intelligence for anomaly detection in video surveillance address some of the challenges, largely overlooking the evolving nature of anomalous behaviours over time. In this paper the authors proposed the ISTL method to address the challenges and limitations of anomaly detection and localization for real time video surbeillance ISTL is unsupervised machine learning based deep learning approach that automates the active learning with fuzzy aggregation which continuously update the differences between new anomalies and normality that evolve over time The followed ISTL is used to demonstrate and evaluate on accuracy ,robustness and computational overhead as well as contextual indicators using three bench mark datasets The three bench marks datasets corresponds to three challenges (i) handling high dimensional video surveillance data streams in real-time (ii) formulating the anomaly detection as to

		learn normality (ii) formulating the anomaly detection as to learn normality From a practical perspective of video surveillance, ISTL ensures a human observer is not required to continuously monitor surveillance footage to determine anomalous behaviour
2019	**Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches** **AUTHORS:** MahmudulHasanMd. MilonIslamMd Ishrak IslamZarifM.M.A.Hashem **CITATION:** https://www.sciencedirect.com/science/article/pii/S2542660519300241	In this paper the authors have propose the machine learning based models to detect anomaly detection on IOT sensors in IOT sites . Detecting the anomaly detection in IOT domain become a major concern in now a days , In this present era of increased IOT infrastructure I every domain , threats and attacks has been increased a lot Which leads to data type problems , Malicious control of entire system and denial of service , spying and malicious operation etc .. which leads to IOT system failure . To avoid such situations by users of IOT systems , the authors proposed a machine learning based models to identify and detect the attacka and anomalies of IOT systems The authors used the machine learning (ML) algorithms that have been used here are Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN). Theevaluation metrics used in this comparision of detection are accurate and precised . The system obtained 99.4% test accuracy for Decision Tree, Random Forest, and ANN. Despite the fact that these strategies are equally accurate, other measurements

		show that Random Forest outperforms them.
2019	**Anomalous Rule Detection using Machine Learning in Software Defined Networks** **AUTHORS:** Vignesh Sridharan, Mohan Gurusamy and Alberto Leon-Garcia **CITATION:** https://ieeexplore.ieee.org/abstract/document/9039984	The authors have proposed a Machine Learning (ML)-based framework for finding anomalies due to malicious rules imposed by a vulnerable controller and identifying damaged control. And also developed a Machine learning based detection Technique for Anomaly Detection in SDN (MTADS) as part of framework that detects complex behaviors to identify and model aspects of transmission rules that can be a sign of a flow table and existing rules. Authors use network operator link. The proposed acquisition framework frame work is based on MTADS. The ML-based acquisition module, MTADS, is based on DBSCAN technology, which is an unregulated machine learning method. They have used this process as DBSCAN is very resistant to outsiders present in the training database. The following elements are included to indicate the rule: Action, Number of Similar Fields, Duration of Duration, Disable / Hard Closure, Source and IP Location, Address, Traffic Costs. To mark the overall flow table, the following factors are considered: Rule Number, Total Number of Bytes Transferred and Received, Byte Packet Number, Number. Bytes Transferred and Accepted in Each Thread. All features are standardized and rated accordingly. Performance of MTADS, Detection Rate for Each Attack MTADS-D, Distribution Specificity was clearly defined using

		graphs. The proposed study provides better information on Uncertainty Laws Acquisition using Machine Learning in Defined Software Networks. The machine learning is more effective and efficient.
2019	**Detection of Anomalies in the Information Networks of Industrial Automation Systems Based on Artificial Immune Detectors** **AUTHORS:** Vyacheslav Tokarev Alexey Sychugov Alexander Anchishkin **CITATION:** https://ieeexplore.ieee.org/abstract/document/8867593	The proposed detection system is based on the creation and training of immune detectors based on the adaptation of sensory networks. AI strategies are defined to improve the security of Information Systems in the realm of the discovery of bizarre behaviors. In this article an immune detector built on the basis of a self-regulating neural network (Kohonen layer) with disrupted neurons, architecture and immune detectors developed on the basis of Markov hidden models (HMM detectors) were investigated. The Kohonen-based IDS has shown better results for the immune system, based on the hidden Markov model. In order to improve acquisition quality, and to make ADS more flexible and adaptable, the confusing network parameters are maintained and recorded in the training sample, thus adding the latest data to it. The input data contains 41 network application parameters, consisting of 4 standard ones. 37. The performance of the proposed ADS, a confusing software based on network traffic, was developed by them. The results of this program were compared with the results of other IDS. The system quality check was performed on the KDD Cup 99 function. This result is due to the very difficult task of preparing the data for analysis, and later the

		accuracy percentage can be improved
2019	**Effective and efficient network anomaly detection system using machine learning algorithm.** **AUTHORS:** Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn **Citation:** http://journal.portalgaruda.org/index.php/EEI/article/view/1387	A network anomaly detection system allows you to monitor a computer network that doesn't follow the network protocol, and it's used in a variety of settings. However, when distinct application domains have different defining abnormalities in their environment, the problem occurs. Thus, using the UNSW-NB15 dataset to compare their performance in terms of accuracy (effective) and processing time (efficient) for a classifier to develop a model, supervised Machine Learning (ML) is utilized for network anomaly detection system with low communication cost and network band width. **Implementation Framework:** 1. Evaluate the best ML algorithm for anomaly detection. 2. There are five classification algorithms used in this experiment includes Naïve Bayes (NB), Averaged One Dependence Estimator (AODE), Radial Basis Function Network (RBFN), Multi-Layer Perceptron (MLP), and J48 trees. 3. Distributed algorithm for network anomaly detection system 4. In the context of ML approaches, training and testing is compulsory to be applied. In a distributed algorithm, the decision is made by selecting available nodes in the network system at random in order to amplify the collected data and quantify the predicted outcome. The result of accuracy computed based on the following formula in for evaluating intelligent algorithms:

		$Accuracy\ (\%) =(TP+TN\ /N\ )X\ 100\%$ TP=correctly predicted as attacks TN=correctly predicted as normal N=Total number of instances **Applications:** 1. Classification rate(accuracy): Different applications domains have different viewpoint about anomalies and this cause the different ML algorithm might well suited for anomaly detection. 2. Time: Time is very important and necessary when dealing a build network anomaly detection system. 3. Comparison: By designing a distributed algorithm and this case we only built a distributed AODE algorithm which is an effective and efficient for anomaly detection that proved. **Conclusion:** To summarize, the machine learning method to classification is more effective, efficient, relevant, and high performing. Moreover, distributed AODE algorithm overcome the issue of centralization when the finding showed the considerably result although a little drop of accuracy and a bit longer time needed. As the performance of distributed batch ML algorithm is surprisingly taking longer. Therefore, to improve it by designing a distributed algorithm using online learning instead of batch learning that take time during training stage.
2019	**Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture**	The number of phishing attacks has increased, exceeding the operational skills of cybersecurity analysts. To increase threat detection response times, the cognitive security application suggests the use of

	AUTHORS: Ivan Oritz Graces; Maria Fernada Cazares; Roberto Omar Andrade **Citation:** https://ieeexplore.ieee.org/abstract/document/9070902/authors#authors	bigdata, machine learning, and data analytics. This study examines the examination of unusual behaviour associated with phishing web attacks, as well as how machine learning approaches might be used to combat the problem. Phishing attacks attempt to obtain information about someone or something, therefore it is vital to develop tools to assist people, particularly security analysts, in dealing with such assault. AI is one of these possible solutions, it can help to detect anomalous behavior, but even better AI can offer new possibilities to protect sensible information, and it is capable to detect anomalous behavior quickly; this is why is so important in new cybersecurity approaches. **Implementation Framework:** People are attempting to implement programmes where computers can take decisions instead of humans due to new trends for possible solutions to detect anomalous behaviour using AI-based techniques; machine learning algorithms are becoming popular, and people are attempting to implement programmes where computers can take decisions instead of humans, implying that this will be an automatic process and that information, decisions, and incident response will be faster than in previous years. **Applications with Machine Learning:** Develop machine learning algorithms. Machine learning has different ways, so here we will discuss about how useful are Logistic Regression and Neural Networks

		for detecting anomalous behavior. 1. Logistic Regression: Is used in classification process. 2. Artificial Neural Network: ANNs can be used when there is little knowledge of the relationships between attributes and classes, are suitable for continuous value inputs and outputs. **Conclusion:** Anomalous behavior is a common problem as we saw. • AI is an effective tool for dealing with this unusual behaviour since it is more efficient. • Some phishing strategies, such as shortening URLs, may be detected by technologies such as this machine learning application, which can determine whether a URL is good or harmful. • Machine learning may not always be correct, we can check those URLs in a web checker for URL shortening. • It's best not to open a shortened URL without first checking it, because we already know that many of them contain phishing attempts, malware, and other threats.
2021	**Health Monitoring of Air Compressors Using Reconstruction-Based Deep Learning for Anomaly Detection with Increased Transparency.** **AUTHORS:** Gribbestad, M.; Hassan, M.U.; Hameed, I.A.; Sundli, K. Published: 8 January	This article compares and contrasts several reconstruction-based deep learning algorithms for detecting anomalies in air compressors. The author explains Six different types of deep learning models applied for anomaly detection. Anomalies in such systems are not isolated events, but rather a progressive departure from the norm as the system's components deteriorate. A descriptive range of deviation

	2021 **CITATION:** https://www.mdpi.com/1099-4300/23/1/83	based on reconstruction-based techniques is provided in this study. The majority of anomaly detection methods are black box models that predict whether an event should be classified as an anomaly or not. This study presents a method for improving the transparency and explain ability of reconstruction-based anomaly detection by indicating which system components contribute to the deviation from predicted behaviour.
2021	**Anomaly Detection in Blockchain Networks: A Comprehensive Survey** **AUTHORS:** Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. Published:11 Dec 2021 **CITATION:** https://arxiv.org/abs/2112.06089	In his article, the author discusses all of the fundamentals and preliminaries involved in the field of anomaly detection in blockchain by providing basic background information regarding blockchain technology, anomaly detection, etc. various types of surveys and statistics were gathered using the blockchain technology by the authors. Satoshi Nakamoto was the first to introduce blockchain technology to solve the problem of double spending in Bitcoin as a distributed decentralized ledger. In the past decade, blockchain technology has attracted a lot of attention from industry and academia since it can be integrated with a wide variety of everyday applications based on the latest features of modern information and communication technologies (ICT). **Types of Anomalous Attacks on Blockchain:** 1) Malicious Transaction Pattern Detection 2) Double Spending Detection 3) Money Mixing Detection etc… At last authors conclude the article by highlighting certain vital challenges nearby

		examining that how they can serve as a future researcher in this field. **Ex:** privacy preservation is big challenge
2021	**“Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives”** **AUTHORS:** Yassine Himeur, Khalida Ghanem, Abdullah Alsalemi, Faycal Bensaali, Abbes Amira **Citation:** https://www.sciencedirect.com/science/article/pii/S0306261921001409	This paper provides an in-depth review of existing anomaly detection frameworks for building energy consumption based on artificial intelligence in this regard. In particular, an extensive survey is presented, in which a comprehensive taxonomy is introduced to classify existing algorithms based on different modules and parameters used, such as machine learning algorithms, feature extraction approaches, and anomaly detection algorithms. Sub-meters and smart sensors installed in residential buildings generate massive amounts of data every day. That data, if properly leveraged, could help end-users, energy producers, and utility companies detect anomalous power consumption and understand the causes of each anomaly. As a result, anomaly detection could prevent a minor problem from becoming overwhelming. Furthermore, it will help to improve decision-making in order to reduce wasted energy and promote sustainable and energy-efficient behaviour. IMPLEMENTATION FARAMEWORK: ◊**Clustering:** It is a machine learning scheme that divides power consumption data into different clusters and thus aids in classifying them as normal or abnormal in unlabeled datasets. ◊**One-class classification:** One-class learning (OCL) is based on categorising initial power consumption patterns into two groups: positive (normal) and negative (abnormal)

		◊Dimensionality reduction: Dimensionality reduction can be used as a low-cost classification approach in various machine learning applications because it removes irrelevant power patterns and redundancy. **APPLICATIONS:** 1. Detection of abnormal behavior of end-users: It is the primary application for which anomaly detection has been proposed, with the ultimate goal of reducing wasted energy and promoting sustainable and energy-efficient behaviour. 2. . Detection of faulty appliance: People's lives have become more convenient as a result of the use of various types of appliances in indoor environments. 3. Occupancy detection: Detecting whether a building or one of its components is occupied by end-users is critical for enabling a set of building automation tasks. 4. Non-technical loss detection: It primarily refers to I)detecting unintentional sub-meter malfunctions and electricity theft attacks attempting to bypass sub-meters; (ii) braking and/or stopping sub-meters; (iii) identifying faulty sub-meter records; and (iv) capturing appliances with illegal connections. 5. At-home elderly monitoring: Modern societies face significant challenges in monitoring their elderly people at home. **CONCLUSION:** There has been a systematic and technically informed assessment of anomaly detection systems in building energy usage. presented. A reference-based taxonomy that

		categorises these approaches. Various features such as artificial intelligence have been presented. showed that the majority of anomaly detectio solutions in energy consumption are still in th nascence. Finally, we believe that more research contributions, projects and collaborations with industrial partners should be performed to help anomaly detectio technology reach its entire potential, proving commercial feasibility and facilitating its mainstream adoption in residential buildings.
2021	“**Automatic Detection of Anomalies in Video Surveillance using Artificial Intelligence**” **AUTHORS:** Sreedevi R Krishnan, P Amudha, and S Sivakumari **Citation:** https://www.researchgate.net/publication/350161087_Automatic_Detection_of_Anomalies_in_Video_Surveillance_using_Artificial_Intelligenc	The importance of security in daily life is growing, and thus the use of a video surveillance system is becoming widely accepted in almost all public places. Even though installing surveillance systems in public places will help to identify the perpetrators of the anomalous situation, it will be difficult to do so. Detecting the anomalous situation in real time will assist authorities in minimising the consequences and loss during the anomalous event. The paper proposes an in-depth investigation of various automatic anomaly detection techniques that aid in reducing the loss caused by the anomalous situation. Artificial intelligence advancements aid in the rapid and automatic identification of nominal and anomalous events. The sequential and incremental learning approach to feature extraction will aid in the development of a model that will provide

		more accurate classifications and predictions of anomalies. When using CCTV surveillance, a large amount of video data must be analysed, and dealing with this Big Data is time-consuming. The immediate identification of abnormal events will aid in reducing casualties or even avoiding the situation, thereby enhancing people's security. **Implementation framework:** •The machine can mimic a human being and may have human cognition without being manually coded using artificial intelligence. Artificial intelligence uses a systematic study of algorithms and statistical analysis to create a model with an artificial neural network. •The unsupervised-learning algorithm, Incremental Knowledge Acquisition and Self-Learning (IKASL), uses continuous learning to update the labelled dataset. •The feature space is built using the recorded labels created by Microsoft Cognitive Services API for video frames. **Applications:** The IKASL algorithm has a layered structure of n layers, with learning and generalisation sub-layers in each layer. **◊Continual Learning for Anomaly Detection:** This Machine Learning model will update the Prediction model in a smooth manner using task and data, allowing reuse and retraining of useful knowledge and skills. The use of transfer learning reduces training complexity significantly. The statistical framework for sequential anomaly detection can perform continuous and few-shot video data learning, which aids in the evaluation of video anomaly detection datasets and real

		surveillance video inputs. ◊**Smart Processing and Storage Utilisation method in Surveillance System**: To distinguish anomalous practises from ordinary conduct, the characteristics of criminal behaviour are studied and recorded based on previous experiences**.** ◊**Unsupervised learning and Knowledge Attaining in Surveillance System:** Characterization and automatic labelling of videos based on semantic matters can be performed using Microsoft Cognitive Service. **Conclusion:** • The smart security system can work more efficiently and effectively by implementing a reliable model for automatic Anomaly Detection. Neural Network applications are rapidly evolving, with more to be discovered in the areas of computer vision and automatic anomaly detection in real-time videos. • This paper investigates some of the novel techniques used in a video surveillance system for automatic anomaly detection. This paper discusses a comprehensive description of various Anomaly Detection Methods that exist in real-time video streaming. •. A fast and novel model that uses previously learned knowledge as well as continuously learned knowledge is required for anomaly detection in real-time video streaming. Novel techniques in Neural Networks are an elegant solution for developing a fast and automatic model.

		•The Convolutional LSTM can be used to solve sequence prediction problems involving spatial inputs such as images or video. A given frame can be used to generate an internal scene representation by Generative Adversarial Networks. Another popular neural network used in real-time video anomaly detection is the Convolutional Autoencoder (CAE).
2020	**"A Survey on The Accuracy of MachineLearning Techniques for Intrusion and Anomaly Detection on Public Data Sets."** **AUTHORS:** Rizal Tjut Adek, Munirul Ula **Citation:** https://scholar.google.com/scholar?start=20&q=anomalous+behaviour+of+artificial+intelligence+and+machine+learning+in+information+security+system&hl=en&as_sdt=0,5#d=gs_qabs&u=%23p%3D2nF_rbxIeLUJ	Machine learning can be used to provide analytical-based approaches for attack detection and response in a variety of domains of information security. Officer of security may benefit from machine-learning-based detection and analysis tools Methods of learning However, the precision of these methods is questionable. This research begins with the presentation of an original taxonomy of machine learning approaches. The Machine Learning algorithms were then applied to intrusion detection, emphasising the accuracy as well as the limitations of the methods for detecting attackers. This paper is organised as follows: Section 2 will discuss the research method used in this study. In summarising the findings, this study employs a systematic literature review (SLR). The SLR is a well-known method for gaining a better understanding of the available literatures in the field of machine learning research in information security. **IMPLEMENTATION FARAMEWORK:** •Artificial Neural Networks (ANN) is a method of how computers can learn and recognize something. This is a representation of biological neural

		networks in human brain. In biological neural networks, there is a very wide network, which consists of interconnected neurons. • . To implement the addition of information carried out by SOMA on biological neural networks, at ANN, each layer has a certain weight, which will also always be added together • One of the new machine learning methods is the Convolutional Neural Network (CNN). • CNNs use on 2-dimensional data in the analysis, therefore, the input data should be in be in matrices form. The convolutional layer is used for extracting local features in the matrices data; the pooling layer is responsible for dimension reduction to enhance the feature generalizability and the connected layer is similar to the traditional neural network portion and is used to output the desired result **APPLICATIONS:** Bayesian Network: The normal or attack decision in the detecting intruder and anomaly activity stage has an 88 percent accuracy on the normal and an 89 percent accuracy on the attack categories. Clustering: A correlation analysis is used to select features from the KDD data set. During data pre-processing, a 10% attack-to-no-attack ratio is set. The reported performance for attack or no-attack detection is 98 percent.

		Decision Trees: Compare the performance of Snort and the decision-tree method to summarise the results. This study was also carried out by increasing the number of rules in Snort 2.0 from 150 to 1581. Hidden Markov Models: investigation into detecting XSS and SQL-Injection attacks on web applications HMMs are employed in the extraction of attack signatures. According to the study, 50 percent of the discovered vulnerabilities in 2009 affected web applications. Ariu's study also used the DARPA 1999 data set as well as some other HTTP data sets in the experiment section. The majority of the experiments **CONCLUSION:** This study expands on the literature review of Machine Learning techniques used for information security applications, with a particular emphasis on the accuracy of machine learning methods in intrusion and anomaly detection in public data sets. The following question arises: Which Machine learning methods have high accuracy for detecting anomaly activities Among the machine learning algorithms, for anomaly detectors, \sone-class SVMs perform well and should be an option in future research. One of the most important aspects of a Machine Learning application for security intrusion detection is data availability. It requires appropriate data for training and detection; machine learning techniques

		cannot function without representative data, and obtaining such data sets is difficult and time consuming. The major issues discovered in some research studies are related to data sets. The majority of machine learning applications made use of public data sets, specifically DARPA 1998 and KDD 1999. The KDD 1999 corrected data set is currently the best available data set.
2021	**"A STUDY OF MACHINE LEARNING CLASSIFIERS FOR ANOMALY-BASED MOBILE BOTNET DETECTION"** **AUTHORS:** Ali Feizolla1,Nor Badrul Anuar, Rosli Salleh,Fairuz Amalina,Ra'uf Ridzuan Ma'arof, Shahaboddin Shamshirband **Citation:** https://scholar.google.com/scholar?start=30&q=anomalous+behaviour+of+artificial+intelligence+and+machine+learning+in+information+security+system&hl=en&as_sdt=0,5#d=gs_qabs&u=%23p%3DzPSggtFTJA8J	Mobile devices have become almost ubiquitous in recent years. They are used for more than just making phone calls. Android is the most popular mobile operating system due to its availability as an open source operating system. Because of the proliferation of Android malwares, it is critical to research the best classifiers that can detect these malwares effectively and accurately by selecting the most appropriate network traffic features and conducting a thorough comparison with related works. Furthermore, the rapidly growing rich mobile applications with overwhelming user experiences, such as maps and GPS functions, increase the appeal of mobile devices to users. Certain sensitive data, such as contact lists, passwords, and credit card numbers, are stored on mobile devices as part of their use. Based on this scenario, hackers have turned their attention to mobile devices, where they can obtain an abundance of their desired data, and where security issues are taken less seriously. **Implementation framework:** •In order to combat the malware's rapid growth, this paper aims to investigate the

		best classifier for detecting Android malware using machine learning classifiers .•The study workflow is depicted in detail in Fig 1. There are three major processes: data collection (which includes both normal and infected traffic), feature selection and extraction, and machine learning classifiers. Normal and infected traffic are collected separately during the data collection process. •The selected network characteristics are extracted for inspection by the classifier in the following process. After that, normal and infected data are combined, randomised, and labelled. Finally, the prepared dataset is fed to 5 classifiers, and the results are compared to two related works. •When a device is infected, the bot (malware) contacts the Botmaster and informs him that the device has been successfully infected. There are three methods for connecting a bot to its Botmaster. To begin, a chat server can be specified to make the connection in such a way that the bot and a Botmaster can log in and communicate as if they were two people. Second, a command and control (C&C) server serves as a conduit between the bot and the Botmaster. **Applications:** Only three network traffic features were chosen from a large number of options. The processing power and processing time increase as the number of selected features increases. The following are the features: Connection duration: this specifies how long a connection will last. In theory, a http-based bot is not

		always connected to the server. It connects to the server at regular intervals to see if there is a new command from the hacker (botmaster). As a result, the majority of communications consist of simple handshakes, which is a plausible feature for malware detection. TCP size: stealing user information and sending it to a hacker is one of the most important functions of a mobile bot. TCP payload includes mobile device data that is distinguishable from other packets for this purpose. As a result, TCP size was chosen for this work. • The number of parameters in a GET/POST request: The GET and POST methods in the HTTP protocol are used to send data from the client to the server. They should not be taken literally as English words. For example, Figure 2 depicts a POST method used by Geinimi malware on a mobile device to leak user data to a command and control server. **Conclusion:** •Millions of people around the world use mobile devices. Contact lists, passwords, and credit card numbers are among the sensitive data stored on such devices. Every month, the research community witnesses the emergence of new mobile malware that steals user data and causes numerous problems for the user. In this study, a machine learning approach was used to address mobile device security vulnerabilities. •To detect malicious activities, machine learning classifiers were applied to a mobile device's network traffic. There were five types of classifiers used: Nave Bayes, KNN,

		decision tree, MLP, and SVM. The results are surprisingly good, with KNN detecting 99.94 percent of the time. • This study's data sample is one of the most recent in the research community. However, with the introduction of new malware every month, it is critical to collect malware samples on a regular basis and to analyse and improve security systems. • Alternatively, the same process can be applied to the entire data sample, whereas this study was limited to 10% of the sample. Furthermore, additional network attributes should be used in future works to more thoroughly inspect network traffic. • It is important to emphasise that the goal of this work is to investigate and evaluate various machine learning classifiers for mobile malware detection in order to address the problem of malware proliferation. System performance measurements in intrusion detection and response studies include detection rate (i.e. true positive and false positive rates), precision, and recall.