International Journal of Engineering Science Invention Research & Development; Vol. 5, Issue 6, December 2018
www.ijesird.com, E-ISSN: 2349-6185

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: APPLICATIONS OF MACHINE LEARNING IN INTRUSION AND ANOMALY DETECTION

Dr. Abhijit Gupta[#], Dr. Shreedhar Marasini[*]
[#]*Young Minds Creation, Kathmandu, Nepal*
[1]abhi@youngminds.com.np, [2]shree@youngminds.com.np

Abstract— **The rapid growth of computer networks and electronic services has increased the need for effective cybersecurity. Traditional security systems mainly depend on known signatures, rules, and manually defined patterns. These approaches are useful for known attacks but may have difficulty detecting new or changing threats. Before 2018, researchers had already investigated artificial intelligence (AI), machine learning (ML), neural networks, genetic algorithms, fuzzy logic, and data-mining methods for improving cybersecurity. This paper reviews the development of these approaches, with particular attention to intrusion and anomaly detection. It also examines the use of ML in malware, phishing, spam, and network traffic classification. The study uses a structured review of literature and a conceptual framework linking cybersecurity data, feature extraction, machine learning, detection, and human response. The analysis shows that ML offered important opportunities for detecting complex and previously unseen patterns, but its practical use depended on data quality, suitable features, trained personnel, computing infrastructure, and control of false alarms. The paper also examines Nepal as a developing-country context and argues that AI-based cybersecurity should be introduced gradually through institutional capacity building, secure infrastructure, data preparation, skilled human resources, and controlled pilot projects.**

Keywords—**Artificial Intelligence, Machine Learning, Cybersecurity, Intrusion Detection, Anomaly Detection, Malware Detection, Nepal**

I. INTRODUCTION

The rapid expansion of computer networks, Internet services, and electronic government systems has created new opportunities for citizens, organizations, and governments. At the same time, it has increased exposure to malware, unauthorized access, phishing, denial-of-service attacks, spam, and other forms of cyber threat. Traditional cybersecurity systems have generally depended on signatures, predefined rules, and known attack patterns. Such methods remain useful, but they may not identify new attacks when the characteristics of the attack are not already known.

Artificial intelligence (AI) provides another approach to this problem. AI includes several methods that can support learning, pattern recognition, classification, reasoning, and automated decision-making. By 2017, machine learning (ML), neural networks, and deep learning had already become important areas of AI research. The 2017 Congressional Research Service overview described ML, deep learning, and neural networks as important AI methods and identified cybersecurity as an application area in which AI could support autonomous detection and decision-making [16].

Cybersecurity is particularly suitable for ML because security systems generate large quantities of data, including network traffic, system logs, user activity, executable files, URLs, and messages. These data can contain patterns associated with normal or malicious behaviour. Earlier research had therefore explored statistical learning, decision trees, support vector machines, clustering, neural networks, genetic algorithms, and fuzzy logic for security detection[1][2][3][4][5][6][7].

The problem, however, is not simply whether an ML algorithm can classify an attack. A practical security system must also produce acceptable false-alarm rates, operate with available data, adapt to changing attacks, and support security personnel.

This paper examines the following research question:

How can machine learning improve cybersecurity detection, and what technical and institutional conditions are required for its practical use, particularly in developing countries such as Nepal?

The objectives are to review pre-2018 ML applications in cybersecurity, identify their major strengths and limitations, develop a conceptual framework for ML-based cybersecurity, and examine the readiness and opportunities of Nepal.

II. LITERATURE REVIEW

A. Artificial Intelligence and Cybersecurity before 2018

Artificial intelligence has a long history in computer science. Early AI systems were largely based on predefined rules and expert knowledge. Later developments placed greater emphasis on statistical learning and the ability of computers to learn patterns from data. By 2017, machine learning had become one of the major approaches within AI, together with neural networks, deep learning, natural language processing, robotics, and computer vision[8]. The 2017 CRS overview also noted that AI applications included spam filtering and cybersecurity, where autonomous detection and decision-making could potentially improve reaction time to threats.

The use of automated methods for cybersecurity predates modern machine learning. Denning proposed an intrusion detection model based on the analysis of abnormal system behaviour [8]. Subsequent studies examined data mining and machine learning as methods for identifying patterns associated with attacks[2]. These developments established the basic idea that security events could be analysed computationally instead of relying entirely on manual investigation.

B. Machine Learning for Intrusion Detection

Intrusion detection became one of the most studied applications of ML in cybersecurity. Intrusion detection systems (IDS) can broadly be divided into misuse or signature-based detection and anomaly-based detection. Misuse detection attempts to identify known attack patterns, whereas anomaly detection attempts to identify behaviour that differs from normal activity.

Buczak and Guven reviewed data-mining and machine-learning approaches for intrusion detection and showed that researchers had investigated decision trees, Bayesian networks, neural networks, support vector machines, clustering, and other techniques[3]. Their work also highlighted important limitations, including the difficulty of obtaining suitable labelled data and the uncertainty of selecting the most effective algorithm for a particular cybersecurity problem. A study by Viegas, Santin, and Oliveira similarly noted that anomaly-based approaches remained largely research-oriented because representative datasets and reliable evaluation methods were difficult to obtain[4].

C. Other Security Applications

ML was not limited to intrusion detection. Researchers had also applied classification techniques to malware, malicious URLs, spam, and other unwanted activities. Malware studies examined static and behavioural characteristics of executable files and used classifiers to distinguish malicious programs from legitimate programs [5]. Ma *et al.* demonstrated that statistical learning could identify malicious websites using lexical and host-based URL characteristics [6].

Spam detection also provided an important example of practical ML classification. Research had investigated machine-learning methods for SMS and other forms of spam detection before 2018 [7]. These applications shared a common structure: data were collected, features were extracted, and a classifier was trained to distinguish legitimate from suspicious objects.

D. Research Gap

The literature shows considerable technical research on ML-based cybersecurity before 2018. However, three problems remained. First, many studies relied on benchmark datasets that did not fully represent operational networks. Second, high classification accuracy did not necessarily mean that a system was useful in practice because false positives could overload security personnel. Third, relatively little attention was given to the institutional and infrastructure requirements for deploying such systems in developing countries.

III. Methodology and Conceptual Framework

This study uses a structured literature-review and conceptual-analysis approach. The review focuses on academic papers, technical reports, and other publicly available research published. The purpose is not to evaluate one particular ML algorithm experimentally but to examine the development, applications, benefits, and limitations of AI-based cybersecurity before the major expansion of AI.

The literature was grouped into four analytical categories: intrusion and anomaly detection; malware, phishing and spam classification; network traffic analysis; and data and operational

challenges. Foundational studies were included where they established concepts that remained important to ML-based cybersecurity research. Particular attention was given to studies using machine learning, neural networks, genetic algorithms, fuzzy logic, and data-mining methods.

Nepal is considered as a contextual case rather than as a source of experimental cybersecurity data. Earlier studies by Gupta, Marasini, and Shakya examined e-government readiness, ICT infrastructure, information-system security, auditing, cloud security, and human resources in Nepal [1][2][9][10][11][12][13][14][15]. These studies provide a basis for considering whether the institutional and technological environment is suitable for advanced cybersecurity technologies. Related work by Marasini and Gupta considers AI applications and challenges in e-government [3].

E. Conceptual Framework

The proposed framework views ML-based cybersecurity as a chain of five components:

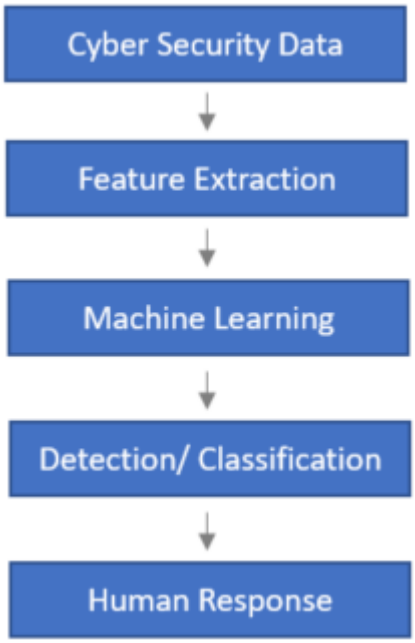

Fig. 1 Chain of five components

This technical chain is supported by four enabling conditions:

1. **Infrastructure** — networks, computing systems, storage, monitoring tools and secure platforms;
2. **Data** — sufficient, relevant, representative and correctly labelled security data;
3. **Human resources** — cybersecurity and ML skills;
4. **Governance** — policies, security controls, privacy, accountability and continuous evaluation.

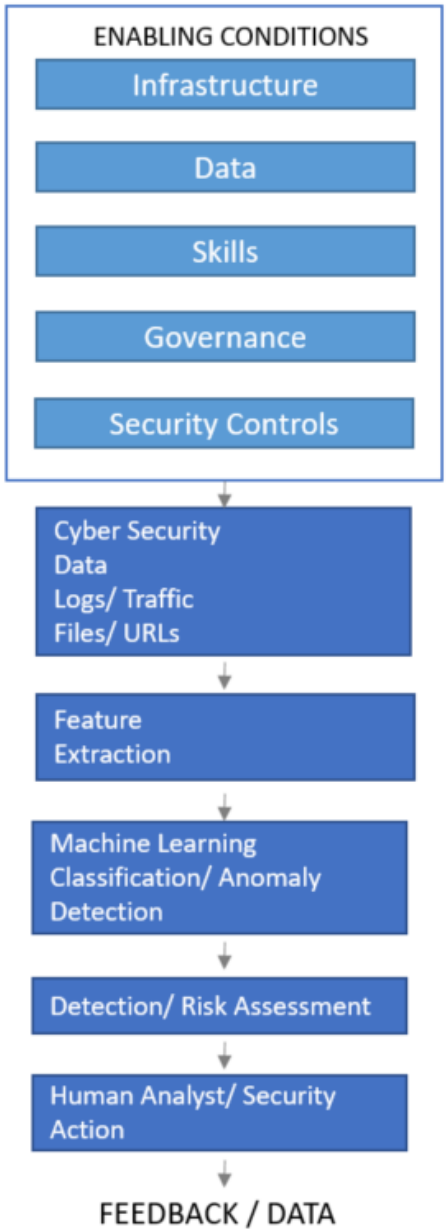

Fig 2. Conceptual Framework for ML-Based Cybersecurity

The framework is useful because it prevents AI adoption from being treated as only an algorithm-selection problem. A technically strong classifier

cannot provide effective protection if the underlying data, infrastructure, skills, or governance are weak.

IV. Machine Learning Applications and Challenges in Cybersecurity

A. Intrusion and Anomaly Detection

Intrusion detection is one of the most important areas in the application of AI to cybersecurity. An IDS attempts to identify activities that may represent unauthorized access, misuse, or attacks. Traditional signature-based IDSs compare observed activity with known attack signatures. This method is effective for previously identified attacks but is less suitable when an attack is new or has been modified.

Anomaly detection provides a different approach. Instead of searching only for known attack signatures, it attempts to model normal behaviour and identify significant deviations. This approach is attractive because an attacker may produce unusual patterns even when the exact attack has not been previously recorded.

Machine learning can support both supervised and unsupervised anomaly detection. In supervised learning, a classifier is trained using labelled examples of normal and malicious activity. Algorithms such as decision trees, support vector machines, Bayesian classifiers, and neural networks have been studied for this purpose [3]. In unsupervised learning, the system works with unlabelled data and attempts to identify clusters or unusual observations.

The choice between these approaches involves a trade-off. Supervised methods can provide strong classification when high-quality labelled data are available. However, obtaining labelled cybersecurity data is difficult because attack data may be limited, sensitive, or expensive to analyse. Unsupervised methods reduce the dependence on labelled data but may generate a larger number of false alarms.

Neural networks offer another approach because they can learn complex relationships between multiple input features. Yin *et al.* proposed a recurrent neural-network-based IDS, showing that neural networks could be applied to sequence-oriented network intrusion data [16].

Other computational-intelligence methods had also been investigated. Genetic algorithms can be used for feature selection and optimisation, reducing the number of variables supplied to a classifier. Fuzzy logic can represent uncertain or gradual conditions, which can be useful when the boundary between normal and abnormal behaviour is not clear.

Table 1. Selected Machine-Learning Approaches for Cybersecurity

Technique	**Typical application**	**Main advantage**	**Main limitation**
Decision tree	Intrusion classification	Easy to interpret	Can overfit
Support vector machine	IDS, malware, phishing	Strong classification capability	Training cost may increase with data
Neural network	IDS, malware	Handles complex patterns	Requires suitable training data
Clustering	Anomaly detection	Does not require complete labels	May produce false alarms
Genetic algorithm	Feature selection, IDS	Useful for optimisation	Computational cost
Fuzzy logic	Anomaly/IDS	Handles uncertainty	Rules may require expert design
Bayesian methods	Classification	Probabilistic interpretation	Depends on assumptions and data

The literature therefore does not support the conclusion that one algorithm is universally superior. Instead, the appropriate method depends on the type of data, attack characteristics, available labels, computing resources, and operational requirements.

B. Malware, Phishing and Spam Classification

Malware, phishing, and spam are different security problems, but they share a common ML structure. In each case, observable features are extracted from an object or event and supplied to a classifier that estimates whether it is legitimate or malicious.

Malware detection traditionally relied heavily on signatures. Signature-based tools work well when a known malware sample has already been analysed. However, new malware, polymorphic malware, and modified versions can make signature-based

detection less effective. ML provides an alternative by learning characteristics of malicious files.

Earlier research examined static features such as byte sequences, executable characteristics, API calls, and other properties [5]. Classification algorithms can then learn relationships between these features and known malware classes. Behaviour-based approaches can also examine program activity during execution.

Phishing detection provides another strong example. Ma *et al.* used statistical methods to classify suspicious URLs based on lexical and host-based characteristics [6]. Their work demonstrated that large numbers of URL-related features could be used to construct predictive models.

Spam detection similarly uses classification. Text, sender information, message frequency, word patterns, and other characteristics can be used to distinguish unwanted messages from legitimate communication. Research on SMS spam before 2018 reviewed a range of machine-learning and hybrid approaches [7].

These applications show an important advantage of ML: the same general classification principle can be adapted to different cybersecurity problems. However, classification performance depends strongly on feature quality and the representativeness of training data.

C. Network Traffic Classification

Network traffic provides a particularly important source of cybersecurity information. A network may generate large numbers of packets and flows, making manual examination difficult. ML can classify traffic according to features such as protocol, packet size, duration, connection frequency, source and destination information, and communication patterns.

Traffic classification can support intrusion detection because abnormal or suspicious traffic may indicate scanning, denial-of-service activity, malware communication, or unauthorized access.

The major challenge is that network behaviour changes over time. A model trained on one environment may perform differently in another environment. For example, normal traffic in a university network may differ significantly from normal traffic in a government data centre.

This problem makes local data important. It also explains why a model with very high accuracy on a benchmark dataset should not automatically be considered ready for operational deployment.

D. Data, Evaluation and Operational Challenges

The quality of training data is one of the most important limitations of ML-based cybersecurity. A model learns from the examples supplied to it. If those examples are incomplete, outdated, unbalanced, or unrealistic, the model may perform poorly in practice.

The KDD Cup 1999 dataset became one of the best-known datasets for intrusion detection research. Later analysis showed substantial redundancy and other problems in the dataset, leading to the development of NSL-KDD as an improved benchmark [17].

This problem is particularly important in cybersecurity because attack behaviour changes. A dataset containing attacks from an earlier period may not represent later attack techniques. Viegas *et al.* specifically highlighted the difficulty of obtaining representative datasets and reliable evaluation methods for real-world anomaly-based intrusion detection [4].

Evaluation must therefore consider more than accuracy. Important measures include:

- **True positive rate:** proportion of actual attacks correctly detected;
- **False positive rate:** proportion of normal activities incorrectly identified as attacks;
- **Precision:** proportion of detected events that are actually malicious;
- **Recall:** proportion of malicious events detected;
- **Detection time:** time required to identify an event;
- **Computational cost:** resources required for analysis.

False positives are especially important in operational environments. If an IDS produces thousands of incorrect alerts, security personnel may ignore genuine warnings. Therefore, a system

with slightly lower accuracy but a manageable false-positive rate may be more useful than a system with high benchmark accuracy but excessive alarms.

Another concern is the changing behaviour of attackers. Once attackers understand the characteristics used by a detection system, they may modify their behaviour to avoid detection. This creates a continuous competition between attackers and defenders.

The main lesson is therefore clear: ML should support cybersecurity analysts rather than be treated as a complete replacement for them.

V. Nepal: Readiness and Opportunities

Nepal provides an interesting case for examining the adoption of AI-based cybersecurity. The country was expanding electronic government services and information systems, but the maturity of ICT infrastructure and institutional capacity varied among government organizations.

Gupta, Marasini, and Shakya examined e-government readiness among ministries of Nepal and identified several dimensions relevant to successful implementation [9]. Their work indicates that readiness cannot be measured only through the availability of computers or Internet connections. Human resources, management, information systems, infrastructure, and security also influence implementation.

Information-system security was another important concern. Gupta and Shakya examined security challenges in Nepal and emphasized the importance of information-system audit and security controls [10]. Their work on information-system auditing in e-government further indicates that security assessment should be considered as part of the wider e-government environment [11]. Cloud computing introduces additional security and governance concerns, particularly where government information systems depend on shared infrastructure and external services [12].

Marasini and Shakya's research on e-government readiness also identifies human resources and infrastructure as important dimensions [14][15]. These findings are directly relevant to AI-based cybersecurity because ML requires both technical infrastructure and skilled personnel.

Table 2.
Nepal's Readiness for ML-Based Cybersecurity

Dimension	**Existing concern**	**Requirement for ML cybersecurity**
Infrastructure	Uneven ICT infrastructure	Reliable networks, servers and storage
Data	Limited security datasets	Centralised and quality-controlled logs
Human resources	Shortage of specialised skills	ML and cybersecurity training
Security	Need for stronger audit and controls	Continuous monitoring and evaluation
Governance	Institutional variation	Clear security responsibilities
Research	Limited local AI research	University-government collaboration
Budget	Competing ICT priorities	Phased investment

Nepal's opportunity is therefore not necessarily to build highly autonomous AI systems immediately. A more practical approach would be to begin with focused applications where ML can support existing security operations.

For example, government organizations could initially apply ML to:

1. network anomaly detection;
2. suspicious URL and phishing detection;
3. malware classification;
4. unusual login detection;
5. spam filtering; and
6. network traffic classification.

These applications do not require replacing existing security controls. Instead, ML can be added as an analytical layer above existing firewalls, antivirus systems, intrusion detection systems, and security logs.

The authors' related work on AI in e-government [13] provides a broader context for considering AI in public-sector systems. However, the present paper argues that AI adoption should be preceded by improvements in the basic security environment identified in earlier Nepal readiness and security studies [9][10][11][12][14][15].

For Nepal, the most important question was therefore not whether AI could theoretically detect cyber threats. International research had already

demonstrated that possibility. The more important question was whether government organizations had sufficient data, infrastructure, skilled personnel, governance, and financial capacity to deploy such systems reliably.

VI. Policy Recommendations

E. Establish a Strong Security and Data Foundation

Government organizations should first improve basic cybersecurity controls. Firewalls, access control, patch management, backup, antivirus, system logging, vulnerability assessment, and security auditing should be established before advanced ML systems are introduced.

ML systems require data. Government agencies should therefore establish secure and standardised logging practices. Network logs, authentication records, system events, malware incidents, and security alerts should be retained in appropriate formats.

F. Develop Cybersecurity and Machine-Learning Skills

AI-based cybersecurity requires people who understand both cybersecurity and data analysis. Nepal should develop training programs covering:

- network security;
- intrusion detection;
- statistics;
- machine learning;
- Python or similar programming languages;
- data preparation;
- security analytics; and
- incident response.

Universities can support this effort by introducing practical research laboratories where students and researchers work with cybersecurity datasets.

G. Establish a Government Cybersecurity Research Laboratory

A national or shared government cybersecurity laboratory could provide a controlled environment for testing ML approaches. The laboratory could maintain anonymised datasets, evaluate algorithms, test detection systems, and develop local benchmarks.

Such a facility would reduce the need for every ministry to independently develop the same capability.

H. Introduce ML Through Controlled Pilot Projects

Government agencies should not attempt to automate all cybersecurity decisions at once. A phased approach is more appropriate.

Table 3.
Suggested Adoption Path

Stage	Main activity
1	Strengthen security controls and logging
2	Collect and standardise security data
3	Develop ML models using historical data
4	Run controlled pilot projects
5	Integrate validated models with security operations
6	Continuously evaluate and update models

Initial projects should focus on high-volume and relatively measurable tasks such as anomaly detection, phishing detection, malware classification, and traffic classification.

I. Improve Digital Literacy and Citizen Protection

Cybersecurity is not only a technical problem. Citizens using electronic government services may be exposed to phishing, fraudulent websites, malicious attachments, password theft, and social engineering.

Government agencies should therefore include cybersecurity awareness in digital-literacy programs. Citizens should be taught how to:

- identify suspicious websites;
- recognise phishing messages;
- use strong passwords;
- protect authentication information;
- avoid unknown attachments;
- verify official government websites; and
- report suspicious online activity.

This can improve both cybersecurity and citizen confidence in electronic services. If citizens do not trust digital government services, technological investment may not result in high adoption.

AI-based security should therefore operate in parallel with public awareness. Machine learning may detect suspicious behaviour, but citizens still need to understand basic security risks.

VII. Discussion

The literature reviewed in this study indicates that machine learning had already become an important research direction in cybersecurity. The field was not new. Researchers had investigated statistical learning, decision trees, neural networks, genetic algorithms, fuzzy logic, clustering, and other computational methods for intrusion detection and related security problems [1][2][3][4][5][6][7][16].

However, the evidence does not support the view that ML had already solved cybersecurity detection. Instead, the research shows a field that was promising but still developing.

Three findings are particularly important.

First, **ML was useful for recognising patterns that were difficult to define through fixed rules**. This was especially relevant for anomaly detection and classification of previously unknown or modified threats.

Second, **data quality was a major constraint**. ML systems require representative data, and cybersecurity datasets are difficult to create because attacks are relatively rare, sensitive, continuously changing, and difficult to label accurately. Research before already recognised this problem[3][4].

Third, **institutional readiness was as important as technical capability**. A government organization may obtain an ML algorithm but still lack the infrastructure, security logs, skilled staff, or governance needed to operate it. This is particularly relevant to developing countries such as Nepal, where earlier studies identified infrastructure, human resources, information systems, and security as important e-government readiness dimensions [9]-[15].

The implication is that AI-based cybersecurity should be viewed as a **socio-technical system**, not simply as software. Its success depends on the interaction between algorithms, data, infrastructure, people, and institutional processes.

VIII. Conclusion

Artificial intelligence and machine learning were already emerging as important cybersecurity technologies. Research had applied ML to intrusion detection, anomaly detection, malware classification, phishing detection, spam filtering, and network traffic analysis. Neural networks, genetic algorithms, fuzzy logic, decision trees, support vector machines, clustering, and other methods had all been investigated.

The review shows that the major value of ML in cybersecurity was its ability to identify patterns in large volumes of data. This capability was particularly important for anomaly detection, where predefined signatures may not be sufficient. The 2017 Congressional Research Service overview also recognised cybersecurity as an important AI application and identified autonomous detection and decision-making as potential benefits [8].

At the same time, significant limitations remained. ML systems depended on suitable training data, feature selection, algorithm design, computing resources, and continuous evaluation. Benchmark performance could not automatically be translated into operational effectiveness. False positives were particularly important because excessive alerts could reduce the value of a security system. Changing attack behaviour also required models to be updated continuously.

The paper's conceptual contribution is a simple framework connecting cybersecurity data, feature extraction, machine learning, detection, and human response, supported by infrastructure, data quality, human resources, and governance. This framework emphasises that AI adoption is not only an algorithmic problem.

The Nepal case further demonstrates this point. Earlier research on Nepal's e-government readiness and information-system security identified infrastructure, human resources, information systems, audit, and security as important implementation factors [9]-[15]. These factors should be strengthened before large-scale AI-based cybersecurity systems are introduced.

The main limitation of this study is that it is based on secondary literature rather than experimental testing using Nepalese government network data. Future research should therefore develop local cybersecurity datasets, test ML algorithms using Nepalese network conditions, compare false-positive rates, and evaluate the operational cost of different approaches. Future studies may also examine how AI can support

national cybersecurity operations while maintaining human oversight, privacy, accountability, and public trust.

The central conclusion is that machine learning was already a promising cybersecurity technology, but its successful adoption required more than algorithms. Data, infrastructure, skilled personnel, governance, and human decision-making were equally important. For Nepal and other developing countries, a gradual and evidence-based adoption strategy would therefore be more appropriate than attempting immediate full automation.

REFERENCES

[1] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering,* Vols. SE-13, no. 12, pp. 222-232, 1987.

[2] W. Lee, S. J. Stolfo and K. W. Mok, "Mining in a data-flow environment: Experience in network intrusion detection," in *5th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining,* San Diego, CA, USA, 1999.

[3] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 2, pp. 1153-1176, 2016.

[4] E. K. Viegas, A. O. Santin and L. S. Oliveira, "Toward a reliable anomaly-based intrusion detection in real-world environments," *Computer Networks,* vol. 127, pp. 200-216, 2017.

[5] R. Moskovitch, D. Stopel, C. Feher, N. Japkowicz and Y. Elovici, "Unknown malcode detection using OPCODE representation," *European Conference on Machine Learning and Knowledge Discovery in Databases,* pp. 204-215, 2008.

[6] J. Ma, L. K. Saul, S. Savage and G. M. Voelker, "Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs," in *15th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining,* Paris, France, 2009.

[7] H. Sajedi, G. Z. Parast and F. Akbari, "SMS spam filtering using machine learning techniques: A survey," *Machine Learning Research,* vol. 1, no. 1, pp. 1-7, 2016.

[8] L. A. Harris, "Overview of Artificial Intelligence," Congressional Research Service, CRS In Focus IF10608, Washington, DC, 2017.

[9] A. Gupta, S. Marasini and S. Shakya, "E-Readiness Assessment for Ministries of Nepal for Implementation of e-Government," *2015 International Conference on Data Mining, Electronics and Information Technology (DMEIT'15) August 10-11, 2015 Pattaya, Thailand,* vol. ERPUB, 2015.

[10] A. Gupta and S. Shakya, "Information System Audit: A study for security and challenges in Nepal," *International Journal of Computer Science and Information Security (IJCSIS),* vol. 13, no. 11, 2015.

[11] A. Gupta and S. Shakya, "Information System Audit: An Overview study in e-government of Nepal," in *IEEE, International Conference of Green Computing and Internet of Things,* Galgotia University, Delhi, 2015.

[12] A. Gupta and S. Shakya, "Information System Audit: Cloud Computing Security and Challenges," *International Journal of Computer Science and Mobile Computing,* vol. 4, no. 11, pp. 48-56, 2015.

[13] S. Marasini and A. Gupta, "Artificial Intelligence in E-Government: Emerging Applications, Opportunities and Challenges," *International Journal of Engineering Science Invention Research & Development,* vol. 5, no. 2, 2018.

[14] S. Marasini and S. Shakya, "E-Readiness to Implement E-Government: An Overview Study in HR Domain in Nepal," in *Proc. IEEE Int. Conf. Green Computing and Internet of Things (ICGCIoT),* Noida, Delhi, 2015.

[15] S. Marasini and S. Shakya, "E-Readiness: A Study of Infrastructure for E-Government of Nepal," *International Journal of Mobile Computing and Computer Science,* vol. 4, no. 12, 2015.

[16] C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural network," *IEEE Access,* vol. 5, pp. 21954-21961, 2017.

[17] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symp. Computational Intelligence for Security and Defense Applications,* Ottawa, ON, Canada, 2009.

[18] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *IEEE Symp. Security and Privacy,* Oakland, CA, USA, 2010.

[19] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Chalmers University of Technology, Göteborg, Sweden, 2000.

[20] E. Eskin, A. Arnold, M. Prerau, M. Portnoy and S. Stolfo, "A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data," *Applications of Data Mining in Computer Security,* pp. 77-101, 2002.

[21] S. Stolfo, W. Fan, W. Lee, A. Prodromidis and P. K. Chan, "Cost-based modeling for fraud and intrusion detection: Results from the JAM project," in *DARPA Information Survivability Conference and Exposition,* 2000.

[22] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection," in *International Journal of Information Security,* 2016.

[23] N. Shone, T. N. Ngoc, V. Dinh and Q. Shi, "A deep learning approach to network intrusion detection," in

IEEE Transactions on Emerging Topics in Computational Intelligence, 2018.