Recent Advances and Applications of Artificial Intelligence and Machine Learning

Recent Advances and Applications of Artificial Intelligence and Machine Learning

Edited by

Raman Kumar

Cambridge Scholars Publishing

Recent Advances and Applications of Artificial Intelligence
and Machine Learning

Edited by Raman Kumar

This book first published 2026

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-0364-6468-4
ISBN (Ebook): 978-1-0364-6469-1

TABLE OF CONTENTS

PREFACE

In recent years, there has been an exponential increase of focus on artificial intelligence and machine learning, including methodologies, theories, tools and techniques underlying this evolving field as well as its potential use in various domains across the entire spectrum of sciences (natural science, health science, engineering, social science, management and humanities) and in various types of businesses. Artificial intelligence and machine learning has not achieved its full potential and is projected to play a significant role in development of successful future intelligent systems.

Recent advances and applications of artificial intelligence and machine learning is an edited book that contains contributions from various experienced professionals ranging from the foundations of multiple disciplines. The book enabled scientists, scholars, engineers, professionals, policy-makers, government and non-government organizations to share new developments in theory, analytical and numerical simulation and modelling, experimentation, operational tests and ongoing developments with relevance to advances in artificial intelligence and machine learning.

The book is divided into two parts comprising four and six chapters, respectively.

The first part The Foundations of Artificial Intelligence is a research area within Computer Science and Engineering that focuses on the development of algorithms that leverage data and statistical tools to solve complex human tasks, to explore novel applications of such tools, and to better understand the apparent success of AI in practice. Instead of focusing on specific applications (e.g., computer vision, NLP or robotics), the Foundations of Artificial Intelligence area focuses on general principles and novel approaches that can be applied across a wide spectrum of applications. We are particularly interested in topics such as machine learning theory, scalable and distributed training, heterogeneity-aware inference, and robust dynamically adaptive algorithms that help navigate multi-dimensional tradeoff spaces spanned by ML accuracy, model size, latency, and spatio-temporal cost efficiency of both training and inference.

The second part incudes Ubiquitous Applications of Artificial Intelligence and Machine Learning Ubiquitous Applications of Artificial Intelligence. Machine Learning and its applications is a pivotal reference source for the latest research on the issues and challenges machines face in

the new millennium. Featuring extensive coverage on relevant areas such as Space for Smart, circular cities, public safety, transportation, mobility computational advertising, software engineering, and bioinformatics, building components, city innovation, intelligent communities, smart destinations, sustainability, system dynamic models, ubiquitous interactive spaces, urban planning, visualization techniques, adaptive websites, affect computing, computational advertising, web-based services and planning. This publication is an ideal resource for academics, graduate students, engineering professionals, and researchers interested in discovering how they can apply these advancements to various disciplines.

This book can benefit researchers, advanced students as well as practitioners. The collection of papers in this book can inspire future researchers in particular, researchers interested in interdisciplinary research. The rich interdisciplinary contents of the book can be of interest to faculty, research communities, researchers and practitioners from diverse disciplines who aspire to create new and innovative research initiatives and ubiquitous applications. This book aims to aspire researchers and practitioners from different research backgrounds regarding new research directions and application domains within artificial intelligence and machine learning.

We wish to thank all of the people who contributed to this edited book. We wish to thank the authors for their insightful contributions, the reviewers for their suggestions that ensured the quality of individual parts and, last but not the least, the Cambridge Scholars Publishing team for their continuous support throughout the project. Without this joint effort, this book would not have been possible.

Kapurthala, Punjab, India
Dr. Raman Kumar

PART 1

CHAPTER 1

FOUNDATIONS OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING USING CRYPTOGRAPHY AND DEVSECOPS CONTRIBUTIONS

RAMAN KUMAR[1]
[1]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
I K GUJRAL PUNJAB TECHNICAL UNIVERSITY, KAPURTHALA,
PUNJAB, INDIA

Abstract

As the digital world advances, cybersecurity is becoming increasingly important to people, businesses, and governments. As our reliance on technology grows, so does the threat landscape, which has increased cyberattacks dramatically. In this paper we have explored various developers in encryption. We have identified novel cybersecurity. Finally we also deliberated the Role of DevSecOps. We have also given the simulative analysis of our proposed work. The final outcomes with efficient approach by improving various parameters are also comprehensively deliberated.

Keywords: Cybersecurity, DevSecOps, Cryptography and Cryptanalytics.

I Introduction

As the digital world advances, cybersecurity is becoming increasingly important to people, businesses, and governments. As our reliance on technology grows, so does the threat landscape, which has increased cyberattacks dramatically. At its foundation, cybersecurity is the defense of programs, systems, and data against such intrusions while maintaining data availability, confidentiality, and integrity.

Cryptography is the foundation of cyber security, using dedicated tools to secure data. This methodology uses mathematical algorithms to scramble the data, keeping it unreadable for unsanctioned personnel. Since this information is susceptible, it must be encrypted during transmission and storage. Cryptography also forms the foundation for many security protocols which in turn facilitates such things as secure communications, authentication, and data integrity. Advances in cryptographic solutions are critical to maintaining security as cyber threats continue to evolve.

While traditional cryptographic methods have been effective, they are increasingly threatened by emerging technologies like quantum computing, which can potentially break widely used cryptographic systems. Additionally, new cybersecurity challenges have arisen that are not adequately addressed in conventional academic research. These include issues related to post-quantum cryptography, advanced threat detection using AIML and combination of blockchain technology.

This research aims to explore recent advancements in cryptography and examine emerging cybersecurity challenges, particularly within the DevSecOps framework. The specific objectives are:

Identifying Novel Cybersecurity: Raising awareness about emerging cybersecurity issues that are not commonly addressed in traditional research, such as advanced threat detection and defense strategies against zero-day attacks.

Identifying Novel Cybersecurity: Raising awareness about emerging cybersecurity issues that are not commonly addressed in traditional research, such as advanced threat detection and defense strategies against zero-day attacks.

II. Literature Review on Cryptographic Advancements and Cybersecurity Challenges

A. Recent Developments in Cryptography

Post-Quantum Cryptography (PQC): The quantum revolution is already threatening the security control framework compared with RSA and ECC, both based on conventional cryptographic systems that are susceptible to quantum attacks. PQC algorithms are being designed to withstand these attacks, which will guarantee the integrity of digital communications. Lattice-Based Cryptography, Code-based and Polynomial Multivariate Cryptography.

Elliptic Curve Cryptography (ECC): ECC provides the cryptography same level of security like classical methods but with a much smaller key

size, making it faster and more used in new crypto protocols. And this efficiency is essential for protecting digital systems and communications.

Blockchain and Cryptographic Proofs: The rise of blockchain technology has introduced new cryptographic proofs, such as zero-knowledge proofs (zk-SNARKs), enhancing privacy and security in decentralized systems.

Fully Homomorphic Encryption (FHE): FHE is an encryption scheme that encrypting and decrypting the data, ensuring confidentiality of information. This new feature is all the more helpful in secure cloud computing and privacy-preserving data analysis.

B. Cybersecurity Challenges in the Modern Era

Quantum Computing: Potential Threat to Traditional Algorithm Eliminated! cyber-security algorithms challenge. This risk is being mitigated by researchers that are working on developing quantum-resistant algorithms.

AI & ML for Detection and Response: The emergence of AI and machine learning into cybersecurity frameworks, has enhanced detection/and response to potential threats. These technologies help systems to detect and respond to cyber threats without much hassle.

Lack of Internet of Things (IoT) Security: With the increased use case in IoT devices, this created another level where vulnerability has been increased. To meet the data integrity and confidentiality security rules, lightweight cryptography combined with elliptic curve technology are used to bring a high level of protection to IoT networks.

Zero Trust Architecture (ZTA): ZTA is a robust security model based on the notion that an implicit trust level without first verifying would only cause exposure for assets, resources and systems. This way the tenant assumes no trust by default, reducing a potential attack footprint.

DevSecOps Integration: DevSecOps is essential for fast identification and fixing of vulnerabilities by inserting security practices into the flow of development with operations. This way it makes security a joint responsibility between dev and ops.

III. Results and Analysis

The results and analysis of proposed hypothesis are as follows:

A. Automated Threat Detection

AI and ML models have revolutionized the cybersecurity scene, as they assist in detecting threats. These models go through terabytes details figure out. characteristics of malicious activity.

B. Example Table: Threat Detection Metrics

Table 1-I Threat Detection Metrics

Metric	Description	Example Values
True Positive Rate	The percentage of real threats system identifies it right	95%
False Positive Rate	The proportion of benign misclassified activities threats	5%
Detection Time	Average time taken to detect a threat after it occurs	30 Seconds
Data Analysed	Volume of data processed for threat detection	1 TB/day

C. Predictive Anylysis

This data can be used by AI and ML to predict potential security incidents organizations may face.

D. Predictive Model Performance

Add a graph with the model metrics over time (accuracy, precision, recall & F1 score) For example, they can be demonstrated in a line or bar chart..

E. Performance metrics over time

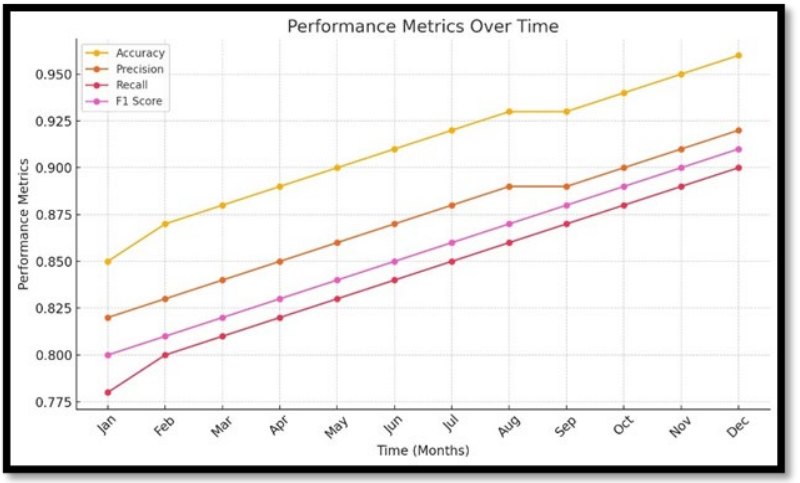

Fig. 1.1 Performance metrics over time

X-axis: Time (months/years)
Y-axis: Performance Analysis / Metrics (F1 Score, Recall, Precision and Accuracy)
Data Points: Reflect metrics over time, that is how much model has improved/degraded on different points in inferences.

IV. Additional Results

We have obtained the following results as listed below:

1. Accuracy: Over year, starting at 85% in January and reaching 96% by December. This indicates correctly identify threats.
2. Precision: Precision also showed a steady increase from 82% to 92%, suggesting that the model became more accurate in identifying true positives among the predicted positives.
3. Recall: The recall metric improved from 78% to 90%, indicating an enhanced capability to detect actual threats over time.
4. F1 Score: The F1 score, which balances precision and recall, improved from 80% to 91%, highlighting the overall effectiveness of the model in threat detection.

Table 1-II Include tables summarizing the monthly performance metrics for a more detailed breakdown.

Month	Accuracy	Precision	Recall	F1 Score
Jan	0.85	0.82	0.78	0.80
Feb	0.87	0.83	0.80	0.81
Mar	0.88	0.85	0.82	0.83
Apr	0.89	0.86	0.83	0.84
May	0.90	0.87	0.84	0.85
Jun	0.91	0.88	0.85	0.86
Jul	0.92	0.89	0.86	0.87
Aug	0.93	0.90	0.87	0.88
Sep	0.94	0.91	0.88	0.89
Oct	0.95	0.92	0.89	0.90
Nov	0.96	0.93	0.90	0.91
Dec	0.97	0.94	0.91	0.92

Lifelong Learning:

Lifelong learning in AI and ML systems ensures continuous adaptation to new threats, including zero-day attacks, by updating their models with fresh data.

Example Diagram: Lifelong Learning Process

You can present a flowchart or diagram illustrating the lifecycle of an AI/ML model in threat detection, including data collection, model training, deployment, and continuous learning.
Example Diagram Elements:

- Data Collection: Gathering new data from network traffic, logs, etc.
- Model Training: Using new data to refine the model
- Model Deployment: Implementing the model in the live environment
- Continuous Learning: Updating the model based on feedback and new threats.

V. Case Study Examples

User Behavior Analytics (UBA): UBA used by monitoring and analyzing user behavior inside the system to discover abnormal patterns which suggests possible abuse such that IT might be dealing with insider threats or compromised accounts.

The key steps in UBA include:

- Collect data: collecting records of access with network traffic.
- Behaviour Profiling: This is a method to create profiles for users, which are based on common behaviors such as login times and access patterns plus data utilization.
- Anomaly Detection: Identifying the unusual data patterns from pre-established profiles using statistical and machine learning models.
- Anomaly Detection Systems: These systems use algorithms to identify deviations from a defined normal behavior. For example, an anomaly detection system might use clustering techniques to identify outliers or machine learning models to predict and flag unusual activities. The results are often visualized using graphs and charts.
- Example Anomaly Detection:
- Data Points: Represent the count of detected anomalies over time, indicating periods of increased suspicious activity.
- Sample Table: Anomalies detected.

Table 1-III Table for UBA Data

User ID	Normal Login Time	Unusual Activity	Action Taken
U1234	09:00-17:00	Login at 02:00	Alert Triggered
U5678	08:00-16:00	Data download > Unusual	Alert Triggered
U9101	11:00-19:00	Multiple Failed Login	Alert Triggered

Performance Metrics: Present a table or graph that contrasts the various models or systems used in behavioral analysis.

Table 1-IV Table for UBA Data

Model Type	Accuracy	Precision	Recall	F1 Score
Statistical Model	78%	80%	75%	77%
MV Classifier	85%	88%	82%	85%
Neural Network	90%	92%	88%	90%

Post-Quantum Cryptography (PQC):

The paper focuses on progress of Quantum-Resistant Cryptographic algorithm development because traditional private and public key systems are endangered from threat against future quantum computing in practical implementation. Notable PQC methods include:

- Lattice-Based Cryptography: This class problems i.e. computationally unapproachable for current classical and quantum computers which means that they can be the foundations of secure cryptographic systems.
- Diagram Explanation: The following diagram illustrates the process of lattice-based cryptography:
- Generate Lattice Basis (B): Create the lattice structure.
- Generate Public Key (A, e): Derive the public key from the lattice basis.
- Generate Secret Key (s): Create the secret key for decryption.
- Encrypt Message (m): Use key
- Decrypt Message (c): Use secret key to decrypt the ciphertext.

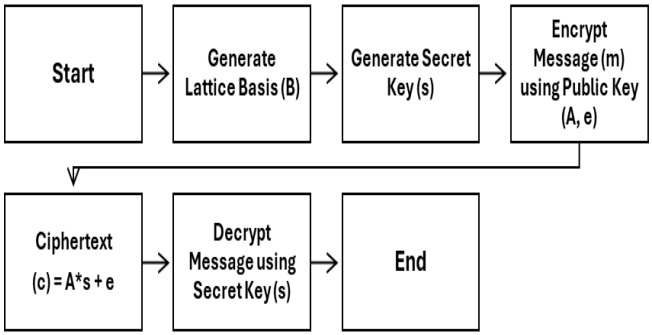

Fig.1-2 Brief description

Table 1-V Comparison of Lattice-Based Cryptographic Algorithms

Algorithm	Security Assumption	Key Size	Encryption Speed	Decryption Speed	Known Attacks
NTRUEncrypt	Shortest Vector Problem	Large	Medium	Medium	Polynomial-time attacks
Learning With Errors (LWE)	Learning with Errors	Moderate	Slow	Slow	Reductions to LWE problems
Ring-LWE	Ring Learning With Errors	Small	Fast	Fast	Reductions to Ring-LWE

Code-Based Cryptography: Error-Correcting Codes for Secure Communications For instance, the McEliece and Niederreiter schemes rely on the supposed hardness of decoding random linear codes.

- Diagram Explanation: The diagram below shows the code-based cryptography process:
- Generate Goppa Code (G, H): Create the error-correcting code.
- Generate Public Key (G, H): Derive the public key from the code.
- Generate Private Key (P, S): Create the private key for decryption.
- Encrypt Message (m): Use the public key to encrypt the message.
- Decrypt Message (c): Use the private key to decrypt the ciphertext.

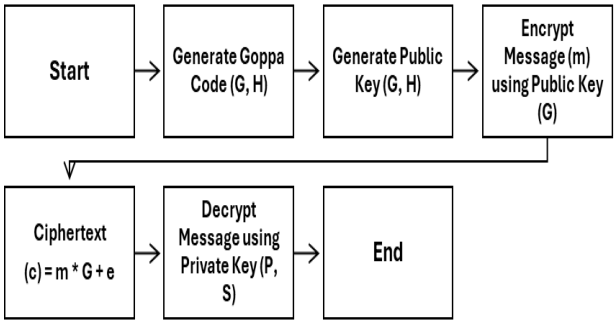

Fig. 1-3 Characteristics of Code-Based Cryptographic Scheme

Table 1-VI Comparison of Lattice-Based Cryptographic Algorithms

Algorithm	Security Assumption	Key Size	Encryption Speed	Decryption Speed	Known Attacks
McEliece	Error Correcting Codes	Large	Fast	Medium	Information set attacks
Niederreiter	Linear Codes and Syndrome Decoding	Large	Medium	Medium	Decoding attacks

Multivariate Polynomial Cryptography:

This consists in solving systems of polynomial equations. UOV (Unbalanced Oil and Vinegar) or Rainbow are schemes like that, because of its complexity and rented in quantum attack.

- Diagram Explanation: The following diagram details the steps involved in multivariate polynomial cryptography:
- Generate Multivariate Polynomial System (P): The polynomial system is generated, which serves as the basis of cryptography and cryptanalysis.
- Generate Public Key (P): The public key is derived from the multivariate polynomial system.
- Generate Private Key (S, T): The private key is created for decrypting messages.
- Encrypt Message (m) using Public Key (P): Generating ciphertext.

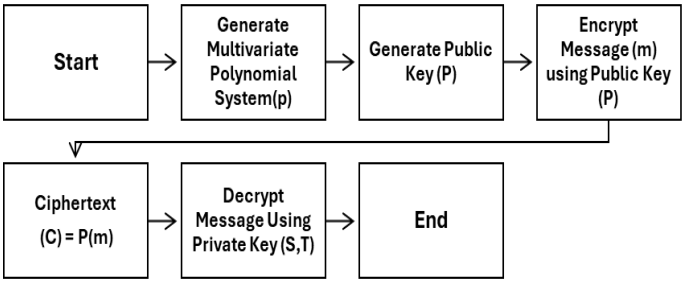

Fig. 1-4 Multivariate Polynomial Cryptography

Table 1-VII Features of Multivariate Polynomial Cryptography

Algorithm	Security Assumption	Key Size	Encryption Speed	Decryption Speed	Known Attacks
Unbalanced Oil and Vinegar (UOV)	Hard Polynomial Systems	Large	Medium	Slow	Polynomial-time attacks
Rainbow	Hard Multivariate Quadratic Systems	Large	Medium	Medium	Reductions to hard problems

Digital Signatures Based on Hash Functions:

There are different approaches to designing a DS based on hash functions, e.g., XMSS and SPHINCS+. Digital signatures and their efficient functioning are possible with the help of hash functions, Merkle trees.

Diagram Explanation: The diagram below outlines the process of creating and verifying digital signatures based on hash functions

1. Generate Public Key (PK) using Hash Functions: The public key is derived from cryptographic hash functions.
2. Generate Private Key (SK) using Hash Functions: The private key is created to be used in the signing process.
3. Signing Message (m) using Private Key (SK): It is used to generating a signature.
4. Signature (σ) = Sign(m, SK): The signature is produced by applying the private key to the message.
5. Verification using Public Key (PK): It ensure authenticity

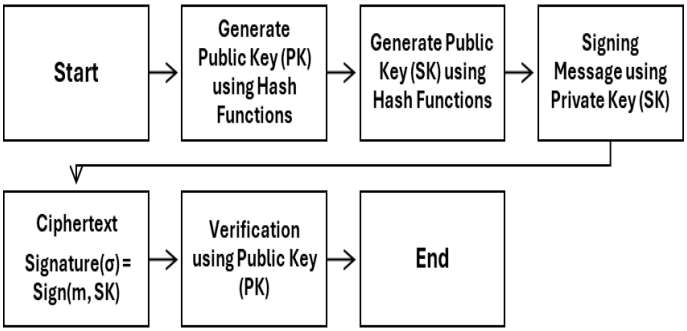

Fig. 1-5 Digital Signature Schemes with Hash Functions

DevSecOps overview:

DevSecOps involves the integration of existing security practices in a given software development lifecycle through DevOps. It ensures shared responsibility from development and operations to IT security. In this case, several tools and techniques are used in DevSecOps to secure an application. Some of the key tools and techniques used in DevSecOps include.

Manual Security Practices

Definition: Manual security work performed by individuals, often encompasses large amounts of time and skill.

Examples:

- Manual code reviews
- Penetration testing
- Threat modeling sessions

Advantages:

- Automated tools may not be able to catch a lot of problematic things skilled humans can.
- Ability to manage unforeseen or complicated cases.
- Disadvantages:
- Labour and time intensive.
- Human error will lead to poor results.

- Large projects are not very scalable.
- Automated Security Practices

Description: Code and security activities executed by tools, integrated in CI/CD.

Examples:

- SAST, DAST Code Scans Automation
- Security testing in CI/CD pipelines
- Real-time Monitoring and Notifications

Advantages:

- Quickly handles large amounts of code
- Consistent - it removes human error and gives consistent results.
- Scalability (a large project with many updates)

Disadvantages:

- Might fail to detect the vulnerabilities that need human judgment, sometimes even if they are not additively complex.
- Prewire and maintenance of automatic tools can be painful.
- If all we rely on is our tools, this could lead to some security issues slipping through the gaps.

Table 1-VIII Table Manual Security Practices vs Automated Security Practices

Aspect	Manual Security Practices	Automated Security Practices
Description	Security activities performed by individuals.	Security activities are performed by tools and scripts.
Examples	- Manual code reviews - Penetration testing - Threat modeling sessions	Automated code scans (SAST, DAST) security testing in CI/CD pipelines, Continuous monitoring and alerting
Speed	Time-consuming and labor-intensive.	Fast, processes large volumes of code quickly.
Consistency	Inconsistent, prone to human error.	Consistent results eliminate human error.

Aspect	Manual Security Practices	Automated Security Practices
Scalability	Not scalable for large projects.	Highly scalable for large projects and frequent updates.
Flexibility	High, can handle unexpected or complex scenarios.	Limited to predefined rules and capabilities of the tools.
Setup and Maintenance	Minimal setup but ongoing high effort.	Complex initial setup, regular maintenance needed.
Expertise Required	Requires significant expertise and experience.	Requires knowledge of tools but less expertise for regular use.
Vulnerability Detection	Can identify complex and subtle issues.	May miss complex vulnerabilities, but quickly finds common issues.
Costs	High due to labor costs and potential for slower processes.	Initial tool costs can be high, but overall ongoing costs.
Example Tools	None (human effort) Custom scripts and manual tools	SonarQube, Checkmarx (SAST) OWASP ZAP, Burp Suite (DAST) Jenkins, GitLab CI (CI/CD) Splunk, ELK Stack (SIEM)
Implementation in CI/CD	Difficult to integrate fully, often separate steps.	Seamlessly integrates into CI/CD pipelines for continuous security.
Output	Detailed reports based on manual analysis.	Automated reports, dashboards, and alerts.
Human Judgment	High, can interpret and understand context-specific issues.	Low, relies on predefined rules and patterns.
Use Cases	Complex threat modeling Penetration testing scenarios requiring creativity	Regular code scanning Continuous integration and deployment security checks Continuous monitoring

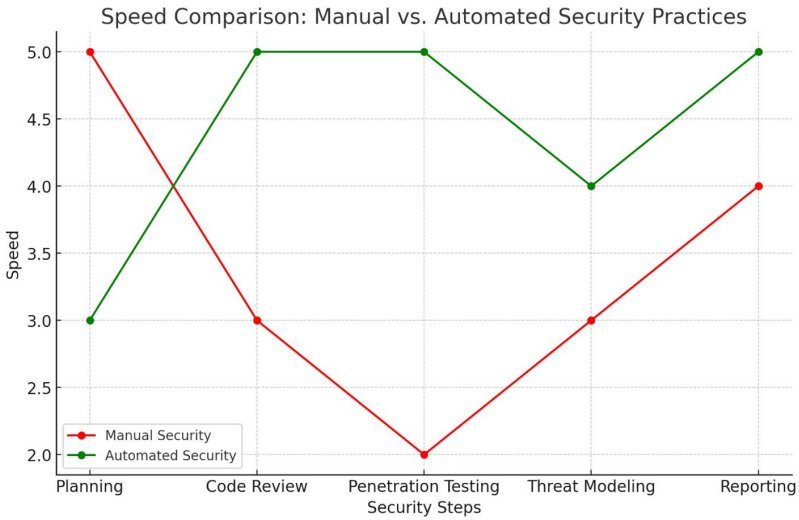

Fig. 1-6 Digital Signature Schemes with Hash Functions

VI. Conclusion

Quantum Computing Threats and Post-Quantum Cryptography (PQC): Discuss the advancements in PQC algorithms, such as lattice-based and multivariate polynomial cryptography, to counter quantum computing threats. Innovations in Encryption: Highlight recent developments, including improvements for better. New Cryptographic Techniques: Cover the progress in secure multi-party computation and fully homomorphic encryption, which allow computations on encrypted data without decryption.

Practical Implications:

DevSecOps Integration: Explore how integrating security practices into development workflows can help identify and mitigate vulnerabilities early in the software development lifecycle.

Blockchain and IoT Security: Discuss the impact of cryptographic advancements on securing blockchain transactions and IoT networks, emphasizing the importance of lightweight cryptography and public key infrastructure.

Limitations and Challenges:

Scalability and Performance: Address the challenges of scaling advanced cryptographic solutions, such as fully homomorphic encryption, for practical use in real-world applications.

Adoption of New Standards: Discuss the slow adoption rate of post-quantum cryptography due to existing infrastructure and the complexity of transitioning from traditional systems.

Future Research Directions:

Exploration of New Algorithms: Suggest further exploration into new cryptographic algorithms that can withstand future technological advancements, including those from quantum computing.

AI and Machine Learning in Cryptography: Encourage research into how AI and machine learning can enhance cryptographic methods and threat detection.

Privacy-Preserving Technologies: Recommend investigations into privacy-preserving techniques, such as zero-knowledge proofs and their applications in various cybersecurity contexts. Include real-world case studies where AI and ML have been successfully implemented for threat detection.

Sample Results:

Increased Anomalies on Specific Days: A noticeable spike in anomalies on weekends, possibly indicating unauthorized access attempts during non-working hours.

Correlation with External Events: Anomalies correlated with major public events, suggesting targeted attacks.

Further Results and Analysis

Detection Accuracy: Highlight the precision and recall rates of the anomaly detection systems. For example, an 85% precision rate with a 90% recall indicates the system is efficient in detecting real threats with minimal false positives.

Case Studies: Include specific examples where UBA successfully identified an insider threat or where anomaly detection systems prevented a potential data breach. Discuss the nature of the threat, the detection process, and the actions taken.

Acknowledgment

The author also wish to thank many anonymous referees for their suggestions to improve this paper.

References

[1] Karenos K., Kalogeraki V., "Traffic management in sensor networks with a mobile sink", IEEE Transactions on parallel and distributed systems, vol 21, issue 10, pp. 1515-1530,2010.

[2] He A., et al., "A Survey of Artificial Intelligence for Cognitive Radios", in IEEE Transactions on Vehicular Technology, vol. 59, no. 4, pp. 1578-1592, May 2010.

[3] Aderohunmu, F. A., and Deng, J. D., "An enhanced stable election protocol (SEP) for clustered heterogeneous WSN," Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, Hong Kong, China, pp.254-258, 2010.

[4] Jiujiu, W., Yuanming, W., and Yanqi, H., "FZCP: A Fixed Zone Clustering Protocol Based on Residual Energy and Nodes Distribution in Heterogeneous Wireless Sensor Networks," IEEE Seventh International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp.1-5, 2011.

[5] Aderohunmu, F. A., Deng, J. D., and Purvis, M. K., "A deterministic energy-efficient clustering protocol for wireless sensor networks," IEEE Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 341-346, 2011.

[6] Jenn-Long Liu and Chinya V. Ravishankar, "LEACH-GA: Genetic Algorithm-Based Energy-Efficient Adaptive Clustering Protocol for Wireless Sensor Networks," International Journal of Machine Learning and Computing, vol.1, no. 1, 2011.

[7] Vijay G., Bdira E. B. A., Ibnkahla M., "Cognition in wireless sensor networks: a perspective", IEEE Sensors Journal, vol 11, issue 3, pp. 582-592, 2011.

[8] Singhal D., Barjatiya S., Ramamurthy G., "A novel network architecture for cognitive wireless sensor network", Proceedings of IEEE International Conference on Communication, Computing and Networking Technologies (ICSCCN), pp. 76–80, 2011.

[9] Karaboga D., Okdem S., Ozturk C., "Cluster based wireless sensor network routing using artificial bee colony algorithm", Wirel. Netw. 18 (7) pp. 847–860, 2012.

[10] Dahnil D. P, Singh Y. P, Ho C. K, "Topology-controlled adaptive clustering for uniformity and increased lifetime in wireless sensor networks", IET Wireless Sensor System,2,pp.318-327, 2012.

[11] Joshi G.P., Nam S. Y., Kim S. W., "Cognitive radio wireless sensor networks: applications, challenges and research trends", Sensors 13 (9) , pp. 11196–11228, 2013.
[12] Mirsadeghi M., Mahani A., "Energy efficient fast predictor for WSN-based target tracking", Ann. Telecommun., 70 (1–2), pp. 63-71, 2015.
[13] Ghaffari A., "An Energy Efficient Routing Protocol for Wireless Sensor Network using A-Star Algorithm," Journal of Applied Research and Technology vol. 12, Issue 4, pages 815-822, 2014.
[14] Abbas N., Nasser Y., Ahmad K. E., "Recent advances on artificial intelligence and learning techniques in cognitive radio networks", EURASIP Journal on Wireless Communications and Networking, 2015.
[15] Anusha S., Mohanraj V., "Dynamic spectrum access in cognitive radio wireless sensor networks using different spectrum sensing techniques", International Journal of Applied Engineering Research, vol 11, no. 6, pp. 4044-4048, 2016.
[16] Gheisari, S., Meybodi, M.R., "LA-CWSN: a learning automata-based cognitive wireless sensor networks", Comput. Commun.,94, 46–56 (2016)

CHAPTER 2

A STUDY FROM TRADITIONAL TO ADVANCED WEATHER FORECASTING MODELS

SUMAN LATA[1] AND AMIT VERMA[2]
[1]RESEARCH SCHOLAR-CSE, MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY, MAHARAJA AGRASEN UNIVERSITY, BADDI-H.P.
[2]ASSISTANT PROFESSOR-CSE, MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY, MAHARAJA AGRASEN UNIVERSITY, BADDI-H.P.

Abstract

For many industries, including mining, agriculture, aviation, and energy production, weather forecasting is essential because it facilitates decision-making and reduces the risks associated with extreme weather occurrences. It also helps in disaster preparedness and public safety. Earlier Weather Forecasting systems were based on conventional statistical weather forecasting techniques and empirical methods. These methods are not accurate for non-linear data set and for big data. With the period of time and advancement in technology better methods using Artificial Intelligence for weather predictions are introduced. These Techniques in result provided better decision making in relation to weather forecasting. This chapter include various ways from earlier method to new weather forecasting techniques. The chapter highlights how artificial intelligence (AI) can revolutionize weather forecasting by combining it with massive data to provide forecasts that are more precise and timelier. These advancements result in more accurate and timely forecasts by imposing complex atmospheric models, real-time satellite data, and automated systems. In addition, the integration of artificial intelligence (AI) and some advanced techniques is enhancing forecast precision by identifying patterns in large datasets that were previously undetectable. Weather estimation has experienced a notable transformation with the

advent of AI and machine learning, moving away from traditional, rule-based models to more data-driven, probabilistic techniques. This chapter looks at how weather forecasting has changed from old methods to modern ones, focusing on the improvements in how accurate forecasts are, how far in advance they can predict, and how they can cover the whole globe.
Keywords: Weather Forecasting, Empirical methods, Artificial Intelligence (AI), Big Data, Real time satellite data, automated systems, data driven, probabilistic techniques.

I Introduction

Predicting the weather in advance allows societies to better prepare for and respond to changing conditions, ultimately saving lives, reducing economic losses, and promoting greater efficiency across various sectors. The ability to accurately predict weather patterns and events—such as thunderstorms, turbulence, high winds, and ice—helps reduce risks, optimize operations, and ensure safety. By predicting areas of disturbance and storms, flight routes can be modified to reduce delays and optimize efficiency. Forecasting helps farmers plan planting and harvesting schedules, reducing crop damage from unexpected weather events [1]. Early warnings for extreme weather like floods, or blizzards allow for better preparation and response [2]. Weather forecasts allow for better route planning in aviation, shipping, and road transport, reducing delays and fuel consumption [3]. Accurate forecasts of solar radiation and wind speeds help energy companies optimize the use of renewable resources, improving grid stability [4] [5]. Predicting weather patterns helps companies plan production and distribution, minimizing weather-related delays. Forecasting wind patterns and temperature helps anticipate pollution levels and alert communities, improving public health outcomes [6] [7].

II Traditional Forecasting Systems

Traditional forecasting systems are still essential for long-term predictions and accuracy based on science [8]. However, by combining these methods with modern AI and machine learning, we can make weather forecasts more precise, faster, and better at adapting to changing conditions.

a) Types of traditional weather forecasting models

Traditional weather forecasting models, such as Numerical Weather Prediction (NWP) models works on difficult mathematical equations and real-time data collected from various sources like weather stations, satellites, ocean buoys, and radar systems [9].

GFS (Global Forecast System) [10] uses sea surface temperature, atmospheric data, snow cover and other observations and integrates all these to forecast patterns globally. Its forecast range from some hours to two weeks. European Centre for Medium-Range Weather Forecasts (ECMWF) model uses satellites observations, weather balloons and earth stations. This model is better known for its accuracy. It uses vast range of meteorological datasets and produces forecasts for the medium-range (from 1 to 10 days) [11]. Another traditional model is Unified Model based on radar data and global datasets. This model combines both short and medium term weather estimations [12].

WRF (Weather Research and Forecasting) Model provides information from global to very localized regions. WRF is widely used in weather research and operational predictions. Another model HIRLAM (High-Resolution Limited area Model) sues regional data, data from satellite and from upper air surroundings. Various European countries uses this model for short-term forecasts as it provides very good accuracy. It can predict up to 3-days weather in advance [13] [14]. COSMO is a regional weather prediction model widely used by several central European countries. This model primarily focuses on providing short-term, high-resolution forecasts with an emphasis on localized weather predictions. To achieve this, it relies on a variety of high-frequency observational data, including inputs from ground-based stations, weather balloons, and radar systems. The model is renowned for its ability to produce detailed weather forecasts, especially in small-scale weather events such as severe thunderstorms or localized rainfall. Its forecast range typically spans from a few hours to up to two days, offering critical data for immediate weather forecasting. The key strength of COSMO lies in its high spatial resolution, making it particularly effective for tracking and predicting smaller weather phenomena [15].

The Fifth Generation Mesoscale Model (MM5) model, developed by the National Center for Atmospheric Research (NCAR) in the U.S., is an older yet still-relevant tool in the field of weather prediction. This mesoscale model specializes in simulating smaller-scale atmospheric phenomena, including storms and localized wind systems. It incorporates a variety of data from weather stations, satellites, and radar to create its predictions. Although MM5, this model is outdated, still it continues to be used for specialized research and for forecasting severe weather events