2025-26/Volume 2/Issue 1

July-December

KSR
COLLEGE OF ENGINEERING

MAGAZINE

CyberSphere

Computer Science Engineering (Cybersecurity)

K.S.R. COLLEGE OF ENGINEERING

An Autonomous Institution

(Approved by AICTE, Affiliated to Anna University, Accredited by NAAC(A++))

K.S.R. Kalvi Nagar, Tiruchengode–637215, Namakkal District, TamilNadu

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

CYBERSPHERE

TECHNICAL MAGAZINE

ACADEMIC YEAR 2025-2026

Vision and Mission of Institution

Vision

To become a globally renowned institution in Engineering and Management, committed to providing holistic education that fosters innovation and sustainable development.

Mission

IM1 Accomplish value-based quality education through innovative teaching-learning process.

IM2 Enrich Engineering and Managerial Skills through cutting-edge laboratories to meet the demands of global integration.

IM3 Enhance innovation and research to meet the evolving needs of industry, society, and sustainable development.

Vision and Mission of Department

Vision

To produce ethical cyber security technocrat for supporting digital ecosystems and sustainable global development.

Mission

DM1 Deliver quality education in cyber security through Immersive learning.

DM2 Impart interdisciplinary skills to meet global cyber security challenges through State of art Laboratory.

DM3 Foster research, innovation, and ethical practices to promote sustainable digital security.

PEOs and PSOs

Program Educational Objectives(PEOs)

PEO1-	**Core Competency**	Analyze and manage security incidents through effective threat detection and response strategies.
PEO2-	**Professionalism**	Exhibit interdisciplinary skills to address cyber security Challenges with ethical integrity that contribute to global cyber resilience.
PEO3-	**Career Development**	Engage in lifelong learning, research and entrepreneurship to foster innovation and lead advancements in cyber security

Program Specific Outcomes (PSOs)

PSO1-	**Secure System Design**	Design and implement secure systems to protect data and infrastructure from cyber threats.
PSO2-	**Threat Detection and Response**	Detect and respond to cyber threats using modern tools and ensure compliance with relevant standards.

K.S.R. COLLEGE OF ENGINEERING

An Autonomous Institution

Chairman Message

Shri.R.Srinivasan, BBM.,MISTE.,
Chairman, KSR Educational Institutions

"Education is the foundation of a brighter tomorrow, and this magazine reflects the vibrant spirit of our learners."

It brings me immense joy to witness the publication of this edition of the **Cyber security Department Technical Magazine – CYBERSPHERE**. As we stand at the forefront of a digital revolution, it is essential that our students are not only informed but inspired to think critically, innovate responsibly, and act ethically.

At KSR College of Engineering, we have always emphasized the **importance of holistic learning**—where academic excellence is complemented by research, practical experience, and ethical grounding. This magazine is a testament to that vision. It represents the convergence of classroom knowledge and real-world application, aligning perfectly with our mission to **create globally competitive and socially responsible engineers**.

I extend my heartfelt congratulations to the editorial board, contributors, and faculty coordinators for their efforts in bringing this edition to life. I am confident that **CYBERSPHERE 2024** will inspire many young minds and serve as a milestone in our journey towards academic and professional excellence.

With best wishes,
Shri.R.Srinivasan
Chairman, KSR Educational Institutions

K.S.R. COLLEGE OF ENGINEERING

An Autonomous Institution

Dean Message

Dr.M.Venkatesan, M.E.,Ph.D.,
Dean, KSRCE

"Knowledge shared is knowledge multiplied"

I am delighted to extend my warm wishes to the Department of Cyber security for the successful launch of the ***Cybersphere*** magazine. This remarkable initiative stands as a reflection of the department's unwavering commitment to fostering knowledge sharing, innovation, and awareness in the dynamic and ever-evolving field of cyber security.

The insightful contributions from both students and faculty members, as showcased in this magazine, are a true testament to their dedication, creativity, and technical excellence. It is encouraging to see such a platform being established to spotlight emerging trends, thought-provoking perspectives, and real-world applications in cyber security.

I whole heartedly encourage everyone to actively engage with ***Cybersphere***, leveragingit as a valuable medium to share insights, explore new ideas, and collaboratively strengthen the cyber security ecosystem.

My heartfelt congratulations to the entire team behind ***Cybersphere*** for their exceptional efforts and vision.

With best wishes,
Dr.M.Venkatesan
Dean, KSR College of Engineering

K.S.R. COLLEGE OF ENGINEERING

An Autonomous Institution

Principal Message

Dr.P.MeenakshiDevi, M.E.,Ph.D.,
Principal, KSRCE

"It is with immense pride that I present the Cyber security Department magazine"

This edition of **CYBERSPHERE** is not just a compilation of technical articles—it is a mirror reflecting the **intellectual energy, dedication, and innovation** of our students and faculty. In an era where digital threats grow more sophisticated by the day, it is crucial that educational institutions take the lead in preparing a new generation of professionals who can **think critically, act swiftly, and uphold ethical standards** in the face of global cyber security challenges.

We at KSRCE take immense pride in offering an **environment that fosters innovation, interdisciplinary collaboration, and hands-on experience**. Our state-of-the-art laboratories, industry-linked curriculum, and dedicated faculty ensure that students are not only job-ready but also future-ready. This magazine is a living proof of that vision—where students are encouraged to question, explore, and solve real-world problems.

I offer my heartfelt **congratulations to the editorial team**, student authors, and department staff who have contributed to the successful release of this magazine. Your efforts have created a platform for thought leadership, creativity, and technical insight.

Let this magazine serve as a source of **motivation, knowledge, and academic excellence**, and may it inspire all readers to contribute meaningfully to the evolving world of cybersecurity.

With best wishes,
Dr.P.Meenakshi Devi
Principal, KSR College of Engineering

K.S.R. COLLEGE OF ENGINEERING

An Autonomous Institution

CHIEF PATRON

Shri.R.Srinivasan,

Chairman, KSR Educational Institutions

PATRON

Mr.K.S.Sachin,

Vice Chairman, KSR Educational Institutions

ADVISORS

Dr.P.Meenakshi Devi,

Principal, KSR College of Engineering

Mrs.K.Sudha,

HEAD, CSE-CS, KSR College of Engineering

EDITORS

Mr.V.Karthi,M.E

Assistant Professor/CSE-CS

Ms.C.S.Namithasri,IV/CSE-CS

Mr.R.Dharan,III/CSE-CS

Mr.R.Alex,II/CSE-CS

Department of Computer Science and Engineering–Cyber security

Enhancing Web Security Using Machine Learning for Phishing URL Detection

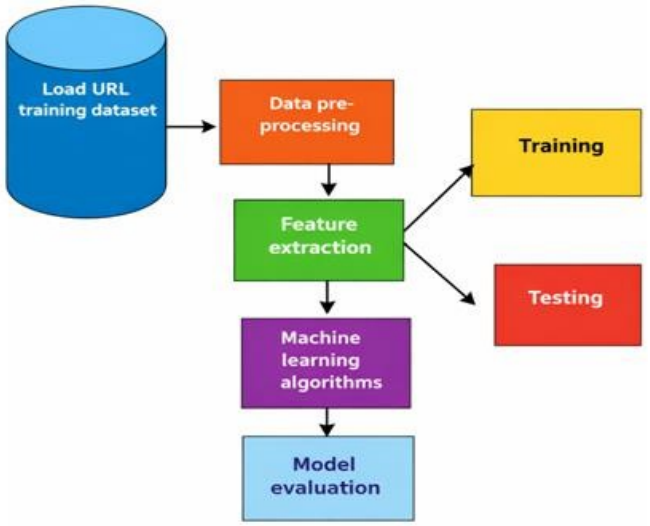
Abstract

To enhance web security by developing a machine learning-based URL detection system that accurately and quickly identifies phishing URLs; this is done for the purpose of reducing phishing attacks and improving online safety. The existing system implies the Support Vector Machine algorithm with10 samples; URL features are processed with convention al machine learning classifiers for phishing detection, often employing techniques of feature extraction and classification. The Proposed system implies the Gradient Boosting algorithm with 10 samples, which combines URL feature pre- processing, TF-IDF for feature extraction and statistical analysis together with an enhanced boosting technique for better phishing URL detection. The proposed system of Phishing URL Detection using the Gradient Boosting algorithm, achieved 92.6% accuracy as compared to the Support Vector Machine algorithm, which had an accuracy of 89.4% and no optimization for speed. The results obtained were statistically significant at a 0.036 level. The Gradient Boosting algorithm exists to have improved detection accuracy and speed in comparison to the Support Vector Machine for phishing URL detection.

Methods

This research study presents web security enhancement in phishing URL detection using a Gradient Boosted model, Cat Boost-an advanced machine-learning algorithm. Model performance comparison carried out on the performance of other Gradient Boosting methods like XG Boost and Light GBM, along with classical methods such as Support Vector Machine (SVM) and Logistic Regression.

It used information extracted from an open platform containing 100,000 URLs labeled as phishing (1) and legitimate (0) with features built on lexical, domain- specific, and host-specific variables.



The process starts with the loading of the URL training dataset, including phishing and legitimate URLs. The first phase of this process is the data pre-processing such as Cleaning and transforming raw URL data to remove inconsistencies and present the information in a format ready for analysis is done in this phase to allow for proper feature extraction. At this point, the next step is feature extraction where by relevant features for the URLs like domain length, presence of special characters, use of HTTPS, and statistical measures concerning the URL text are explored. The Term Frequency-Inverse Document Frequency (TF-IDF) is also applied during this feature extraction phase.

Statistical Analysis

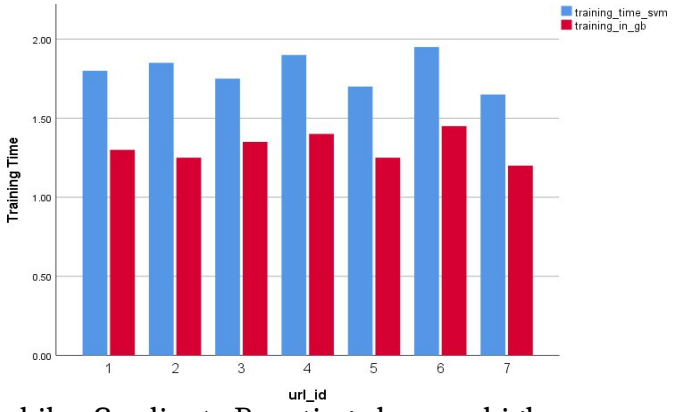
SPSS variant 26.0 was utilized to assess the exhibition of the SVM model in view of accuracy, recall, and detection time. For phishing URL detection, URL features and model type were considered as independent variables, while accuracy, recall, and detection time served as dependent variables.

Result

Performance comparison of the SVM with that of Gradient Boosting models in the detection of phishing URLs brings out some glaring differences.

compare the accuracy, test loss, and training time between the SVM and Gradient Boosting models, SVM model yields accuracy ranging from 84.30% to 89.20% with a loss ranging between 0.74 and.79anda training times of 1.65 to 1.90. But Gradient Boosting performed much better than SVM, it provides accuracies in the range of 88.00% to 94.00%, much lower loss values, and training time of between1.25 and 1.40s. This results in Gradient Boosting being much faster and more accurate in URL phishing detection.

In statistical comparisons, along with independent sample T-tests, were performed on the Gray-Box versus White-Box predictive performance of SVM and Gradient Boosting models. Specifically, a specific set of metrics was used: accuracy, test loss, and training time, in which the mean value, standard deviation, and standard error were calculated across varioussamples.SVM has same an accuracy of 87.356, with a standard deviation of 1.9132,



while Gradient Boosting has a higher mean accuracy of 92.673 with a standard deviation of 2.4006. The test loss for SVM is 0.77, while for Gradient Boosting it is 0.70, indicating good generalization. SVM had a training timeof1.80 second, while Gradient Boosting had a very short training time of only 1.30 seconds. Table 3 Independent samples T-test was performed to compare the accuracy of two models-Support Vector Machine (SVM) and Gradient Boosting (GB).

Comparison

Gradient Boosting has demonstrated an excellent improvement over the traditional phishing URL detection techniques, especially Support Vector Machine (SVM) and other conventional classifiers. Recent research has demonstrated that Gradient Boosting achieved an accuracy of 98.6% significantly

After feature extraction is done, the data set is split into a training set and a test set, with the training data being fed into Gradient Boosting, a very powerful ensemble learning technique that combines weak classifiers to produce better predictive accuracy. This algorithm is very efficient when it comes to detecting phishing URLs because of its capability to decode complex patterns and learn new attacking strategies. Finally, the trained model is assessed on the testing dataset in terms of accuracy, precision, recall, and detection time to ensure generalization against new phishing threats

Outperforming SVM's 92.4%, due to its capability of handling complex lexical, host-based, and content-based features. Another experiment that has utilized ensemble learning with Gradient Boosting and Decision Trees for detecting phishing reported to achieve an accuracy of 97.8% by confirming that the model could indeed differentiate the phishing from a legitimate URL very effectively

Conclusion

The proposed machine-learning system for detecting phishing URLs enhances detection accuracy and speed considerably over traditional methods. By using Gradient Boosting with TF-IDF Feature Extraction and statistical learning methods, the system was able to achieve a very high detection accuracy of 92.6% with a standard deviation of 2. 4006 as compared to a Support Vector Machine- based one. The improvement in detecting phishing would enhance web security by reducing the chances of susceptibility to cyber attacks, which would make the Internet a safer place.

HARIHARAN K
IV- CSE(CS)

Cyber Security – Incident Responder

Abstract
The rapid advancement of information technology and the widespread use of the internet, cyber threats have become a major concern for individuals, organizations, and governments. Organizations today store large amounts of sensitive data such as personal information, financial records, intellectual property, and business secrets in digital form. This increasing dependency on digital systems has made them attractive targets for cyber criminals.

Cyber attacks such as ransom ware, phishing, malware infections, denial-of-service attacks, and data breaches are increasing in frequency and complexity. To defend against these threats, organizations rely on a specialized cyber security team. Among them, Cyber Security Incident Responders play a vital role.

Incident responders are professionals responsible for handling security incidents in a systematic and timely manner. They ensure that cyber attacks are detected early, controlled quickly, and resolved effectively. Their work helps organizations reduce damage, maintain business continuity, and improve overall security posture.

Cyber Security Incidents
A cyber security incident is any event that compromises or threatens the confidentiality, integrity, or availability of information systems or data. These incidents can occur due to external attackers, internal misuse, system vulnerabilities, or human errors.

Types of Cyber Security Incidents
Some common types of cyber security incidents include:

Malware Attacks: Viruses, worms, trojans, and spyware that infect systems.

Ransomware Attacks: Attackers encrypt data and demand ransom for decryption.

Phishing Attacks: Fake emails or messages trick users into revealing credentials

Unauthorized Access: Hackers gain access to systems without permission.

Data Breaches: Sensitive data is stolen or leaked.

Denial of Service (DoS/DDoS): Systems are overloaded to make services unavailable.

Insider Threats: Employees misuse access intentionally or unintentionally

Unauthorized Access: Hackers gain access to systems without permission.

Data Breaches: Sensitive data is stolen or leaked.

Denial of Service (DoS/DDoS): Systems are overloaded to make services unavailable.

Insider Threats: Employees misuse access intentionally or unintentionally.

Incident Analysis
- Analyze logs, system behavior, and network traffic.
- Identify the attack method, entry point, and affected systems.
- Assess the severity and potential impact of the incident.

Incident Containment
- Isolate infected machines from the network.
- Block malicious IP addresses and domains.
- Disable compromised user accounts.

Eradication
- Remove malware and malicious code.
- Fix system vulnerabilities.
- Apply patches and security updates.

Recovery

- Restore systems and data from secure backups.
- Test systems to ensure normal operations.
- Closely monitor systems after recovery.

Incident Response Lifecycle

The Incident Response Lifecycle, as defined by NIST, provides a structured approach to handling incidents.

Preparation

Preparation is the most important phase. It includes:

- Developing incident response policies and procedures.
- Training incident response teams.
- Setting up security tools and monitoring systems.
- Conducting regular drills and simulations.

Identification

In this phase:

- Security alerts are investigated.
- Incidents are confirmed.
- The scope and nature of the incident are identified.

Containment

Containment prevents the incident from spreading further.

- Short-term containment stops the attack immediately.
- Long-term containment applies permanent solutions.

Eradication

This phase removes the root cause of the incident.

- Malware removal.
- Closing security gaps.
- Eliminating attacker access.

Recovery

- Systems are restored to normal operations.
- Services are brought back online.
- Continuous monitoring is performed.

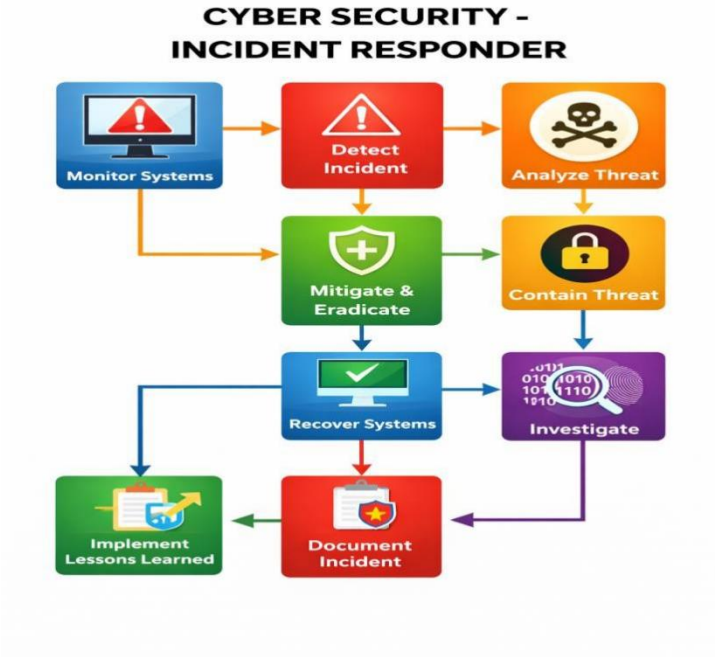
Lessons Learned

Review incident response effectiveness.

- Identify weaknesses.
- Improve future response strategies.

Tools Used by Incident Responders

Incident responders rely on various tools to detect and analyze incidents.



Conclusion

Cyber Security Incident Responders are a critical component of modern cyber security defenses. They protect organizations from cyber threats by responding quickly and effectively to security incidents..

M.GOWTHAM
III-CSE(CS)

Real-Time Cyber Resilience Framework for Smart City IoT Systems

Abstract
Smart cities are no longer experimental concepts they are living, operational systems. Traffic lights respond dynamically to congestion, power grids self-balance demand, water systems automate distribution, and surveillance networks monitor public safety. All of this intelligence is driven by vast, interconnected IoT infrastructures operating continuously and autonomously.

This transformation comes with a harsh reality: smart cities are high-value cyber targets. Unlike traditional IT environments, smart city IoT systems are distributed, heterogeneous, and safety-critical. A successful cyber attack does not merely steal data. It can paralyze transportation, disrupt energy supplies, contaminate water systems, or endanger human lives. In such environments, preventing every attack is unrealistic. Survival, continuity, and rapid recovery become the true measures of security.

From Cyber security to Cyber Resilience
Conventional cyber security strategies emphasize perimeter defense, access control, and breach prevention. These approaches assume that threats can be blocked before damage occurs. In smart city environments, this assumption collapses.
IoT devices often lack:

- Strong authentication mechanisms
- Consistent patching and update cycles
- Sufficient computational resources for heavyweight security controls

As a result, breaches are not hypothetical they are inevitable.
Cyber resilience shifts the focus from How do we stop all attacks to How do we keep the city running when attacks happen.
A real-time cyber resilience framework is designed not only to detect intrusions, but to:

- Absorb the impact of attacks
- Contain their spread
- Maintain essential services
- Recover rapidly without manual intervention

Intelligence Under Pressure: Real-Time Monitoring and Threat Awareness
At the core of cyber resilience lies continuous situational awareness.
The framework operates by monitoring:

- IoT device behavior
- Network traffic patterns
- Sensor data consistency
- System performance anomalies

Instead of relying on static rules, the system learns normal operational baselines for smart city services. Deviations such as unusual communication patterns, data manipulation, or sudden performance degradation are flagged as potential threats in real time.
This behavioral intelligence enables the framework to identify:

- Distributed Denial-of-Service (DDoS) attacks on city networks
- Compromised sensors injecting false data
- Rogue IoT devices impersonating legitimate nodes
- Lateral movement across interconnected city subsystems

Beyond Alerts: Autonomous Response and Impact Containment
Detection alone is useless if response is slow.
A defining feature of the real-time cyber resilience framework is orchestration automated response. When a threat is confirmed, the system reacts without waiting for human intervention.
Response actions include:

- Isolating compromised IoT nodes
- Rerouting traffic away from affected network segments

- Throttling suspicious communication flows
- Activating failover services for critical infrastructure

For example, if a traffic management subsystem is attacked, the framework can isolate the affected sensors while shifting control to redundant nodes, ensuring traffic flow continues safely.

Adaptive Recovery and Restoring Trust After an Attack

Recovery mechanisms include:

- Firmware integrity checks
- Device reauthentication and identity verification
- Trust score recalculation based on behavior history
- Gradual reintegration into the operational network

Architecture of a Real-Time Cyber Resilience Framework

- A typical framework follows a multi-layered architecture:
- **Data Collection Layer**
  Real-time data is gathered from IoT devices, gateways, edge nodes, and control centers.
- **Analysis and Intelligence Layer**
  AI-driven analytics and anomaly detection engines identify deviations from normal behavior.
- **Decision and Response Layer**
  Automated policies determine isolation, mitigation, or failover actions.
- **Recovery and Trust Management Layer**
  Systems validate device integrity and manage reintegration using dynamic trust evaluation.
- **Continuous Learning Layer**
  Attack data is fed back into the system to improve future detection and response accuracy.
  This closed-loop design ensures the framework evolves alongside emerging threats.

Conclusion

The future of smart city security lies in self-healing, self-adaptive urban systems. Technologies such as edge AI, federated learning, and decentralized trust models will further enhance resilience.

SIVAVISHNU A
IV- CSE(CS)

An Intelligent Intrusion Detection System for IoT Networks Using Deep Learning

Abstract

The Internet of Things (IoT) has quietly embedded itself into every layer of modern life—smart homes, healthcare devices, industrial automation, transportation systems, and smart cities. Yet beneath this convenience lies an expanding and largely invisible attack surface. Unlike traditional IT systems, IoT devices are constrained by limited processing power, weak authentication mechanisms, and inconsistent security updates, making them prime targets for cyber attackers.

Conventional intrusion detection mechanisms, designed for enterprise networks, are ill-equipped to defend these dynamic, heterogeneous environments. Static rule-based systems fail to recognize evolving threats, while signature-based detection collapses against zero-day attacks. This gap has given rise to a new paradigm: intelligent intrusion detection powered by deep learning.

From Rules to Reasoning the Evolution of Intrusion Detection

Traditional Intrusion Detection Systems (IDS) rely heavily on predefined rules or known attack signatures. While effective against previously identified threats, these systems struggle with modern attack vectors that continuously mutate to evade detection.

Deep learning fundamentally changes this equation.

By leveraging neural architectures capable of hierarchical feature learning, intelligent IDS models analyze massive volumes of IoT network traffic to uncover subtle, non-obvious attack patterns. Instead of asking "Does this match a known attack?", deep learning asks "Does this behavior deviate from learned normality?"

This shift from rule enforcement to behavioral intelligence marks a turning point in IoT security.

How Deep Learning Strengthens IoT Intrusion Detection

Deep learning–based IDS models are uniquely suited to IoT environments due to their ability to handle complexity and scale.

Key capabilities include:

- **Automatic Feature Extraction:** Eliminates dependence on manual feature engineering.
- **Temporal Awareness:** Recurrent models such as LSTM detect sequential attack behaviors over time.
- **Adaptive Learning:** Models continuously improve as new traffic patterns emerge.
- **Multi-Attack Detection:** Simultaneously identifies DoS, probing, spoofing, and unauthorized access.

System Intelligence: Architecture of a Deep Learning–Based IoT IDS

An intelligent IDS for IoT networks typically follow a layered architecture:

Data Acquisition Layer

Network traffic is collected from IoT devices, gateways, and edge nodes, capturing packet-level and flow-level data.

Preprocessing Layer

Noise removal, normalization, and dimensionality reduction prepare raw data for efficient model training.

Deep Learning Engine

Neural networks—such as CNNs for spatial traffic analysis or LSTMs for sequential patterns—classify traffic as normal or malicious.

Detection and Alert Layer

Identified intrusions trigger alerts, logs, and automated mitigation actions.

Response Layer

The system isolates compromised devices, blocks malicious traffic, or escalates incidents for human intervention.

This architecture enables scalable, real-time protection without overwhelming constrained IoT resources.

IoT-targeted attacks are escalating in both frequency and sophistication.

- **Mirai Botnet:** Hijacked thousands of insecure IoT devices to launch massive DDoS attacks.
- **Healthcare Device Exploits:** Unsecured medical IoT devices exposed patient data and disrupted hospital operations.
- **Industrial IoT Attacks:** Compromised sensors manipulated operational data, causing physical damage.

Limitations and Risks

Despite its advantages, deep learning–based IDS introduce new challenges:

- **Data Bias:** Poorly representative training data can lead to blind spots.
- **Adversarial Attacks:** Attackers may craft inputs designed to deceive neural models.
- **Resource Constraints:** Deploying deep models on low-power IoT devices requires optimization.
- **Explainability:** Black-box decisions complicate trust and forensic analysis.

Addressing these risks requires careful dataset design, adversarial training, and the integration of explainable AI (XAI) techniques.

Preparing for Intelligent Defense

To effectively deploy intelligent IDS in IoT environments, organizations must evolve their security strategies.

Security Teams Must:

- Integrate AI-driven IDS at the network edge.
- Continuously retrain models using live traffic data.
- Simulate attack scenarios to evaluate system resilience.
- Combine human oversight with automated detection.

Conclusion:

As IoT networks continue to expand, the traditional concept of a fixed security perimeter collapses. In its place emerges an intelligent, learning-driven defense strategy.

ASHRAF ALI I
IV- CSE(CS)

Cyber security - State of the art, challenges and future directions

Abstract

Cyber security has become a very critical concern that needs the attention of researchers, academicians, and organizations to confidentially ensure the protection and security of information systems. Due to the increasing demand for digitalization, every individual and organization faces continually shifting cyber threats. This article provides an overview of the state of the art in cyber security, challenges, and tactics, current conditions, and global trends of cyber security. To stay ahead of the curve in cyber security, we conducted a systematic review to uncover the latest trends, challenges, and state-of-the-art in cyber security. Moreover, we address the future direction of cyber security, presenting the possible strategies and approaches to addressing the increasing cyber security threat landscapes, the emerging trends, and innovations like Artificial Intelligence (AI) and machine learning (ML) to detect and automate cyber threat responses. Additionally, this article underlines the importance of ongoing adoption along with collaboration among stakeholders in the cyber ecosystem

Introduction

Advances in information and communication technology and the need for quick access to information have made these tasks more convenient to perform and pose serious security challenges that must be addressed by all stakeholders, from individuals to governments. Due to the advancement of technology security issues may be a risk to individuals, societies, and organizations. To mitigate these security challenges, individuals, organizations, and societies often employ various measures, including cyber security measures, legal frameworks, and education and awareness campaigns to promote ethical behavior and discourage malicious intent. Cyber security is the protection of individuals, societies, organizations, systems, and technologies from abnormal activity. Cyber security is the maintenance of the confidentiality, integrity, and availability (CIA) of computer resources owned by one organization

Application area of cyber security

Cyber security provides confidentiality, integrity, and reliability services for different areas by providing defense mechanisms, intrusion detection mechanisms, and encryption mechanisms

1. Cyber security in smart grid

The smart grid is the next generation of power systems, and by merging cutting-edge computing and communication technologies, it is anticipated to increase the efficiency and dependability of future power systems with renewable energy supplies, distributed intelligence, and demand response.

2. Cyber security in vehicular communication

This includes not only performing regular testing and maintenance of the system but also implementing redundancy and failover mechanisms. Cyber security in-vehicle communications are essential to ensure the security, privacy, and reliability of the system and to maintain the trust of users and stakeholders.

3. Cyber security in smart city

A smart city is an urban area that uses advanced technology and communication infrastructure to improve the quality of life for its citizens. However, the growing reliance on connected systems and devices in smart cities also creates significant cyber security risks that must be addressed to ensure the safety and privacy of citizens and the resilience of critical infrastructure.

4. Cyber security in smart eHealth system

Internet of Things (IoT) -based healthcare applications such as remote patient monitoring, and

smart health rely heavily on internet-connected devices to collect health-related data from various sources such as medical devices and mobile apps.

State of the art

Cyber security provides a defense mechanism for computing systems, networks, and data against unauthorized access, use, or damage and protects society and the economy from online threats that could jeopardize the confidentiality, integrity, and availability of various sectors, including business, government, the military, healthcare, education, and energy

Related work

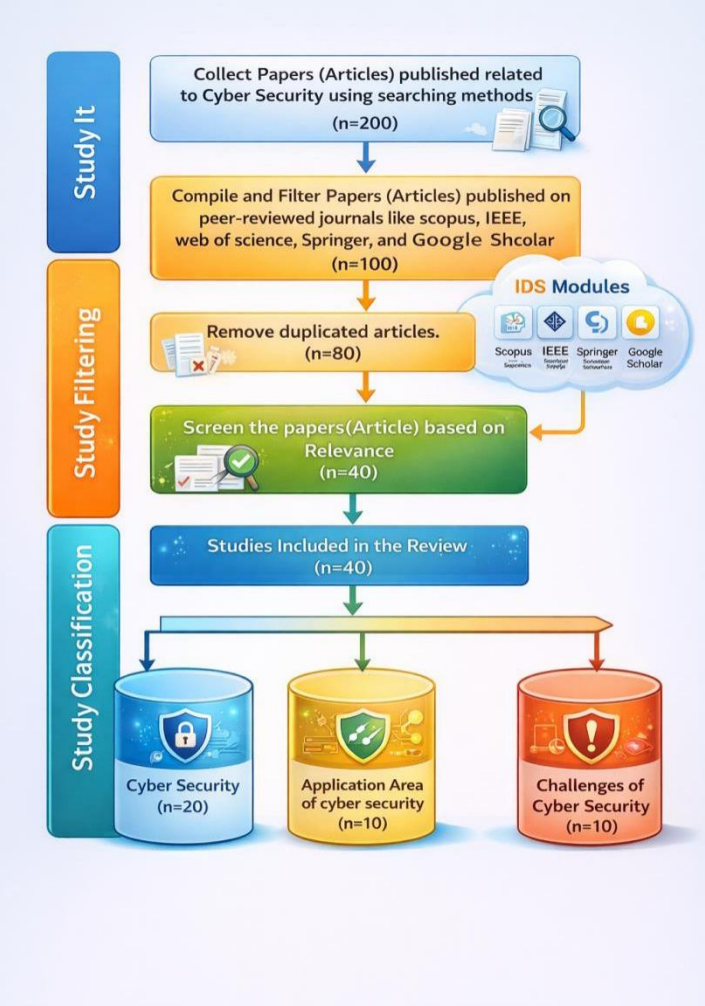
It provides a comprehensive overview of the use of artificial intelligence (AI) in cyber security and discusses the challenges and opportunities of using artificial intelligence (AI) in cyber security. The researcher discusses the potential of Artificial intelligence to address cyber security challenges and the area of AI for cyber security, including the use of artificial intelligence (AI) for anomaly detection, intrusion detection, and malware analysis.

Methodology

This systematic review is conducted based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses statement and the search is conducted from 2013 up to 2023. Due to the large number of papers published in reputable journals, we consider papers published within 10 years.

Challenges of cyber security

In the digital era, cyber security is a critical concern for people, corporations, and governments. With the increased use of technology and digital devices, it is more necessary than ever to secure electronic devices, networks, and data against unwanted access, theft, and damage. With the advancement of technology, the cyber security action of protecting an organization, employees, and critical assets from cyber threats faces several challenges.



Conclusion

Cyber security is essential for protecting the safety of individuals and organizations since highly depend on digital technologies. Cyber security is applicable in different application areas such as health centers financial institutions, smart cities, grid systems, government organizations, education, and the military.

R.ALEX
II CSE-CS

KSR College of Engineering

AN AUTONOMOUS INSTITUTION

NAAC ACCREDITED A++ | NBA ACCREDITED PROGRAMMES

25 YEARS 2001 – 2026 Celebrating Academic Excellence

KSR KALVI NAGAR, TIRUCHENGODE, NAMAKKAL - 637215, TAMILNADU, INDIA.