International Journal On Engineering Technology and Sciences – IJETS
ISSN (P):2349-3968, ISSN (O): 2349-3976 Volume XIII - Issue II, February - 2026

A study paper on Hybrid Cyber security Framework for 5G-Enabled IoT in Smart Cities

[1]Dr. Nazneen Taj, [2]Dhanyashree C.B
[1]Associate professor and HOD, [2]2nd year,
[1,2]Department of Cyber Security, ACSCE, Bangalore.

Abstract

This Research show rapid growth of Internet of Things (IoT) devices and the deployment of 5G networks are transforming traditional cities into highly connected smart cities. While this technological advancement improves efficiency, automation, and public service delivery, it also creates serious cybersecurity challenges. The integration of billions of interconnected devices significantly increases the attack surface, making smart city infrastructure more vulnerable to complex and large-scale cyber threats.

Has Existing traditional security mechanisms are not sufficient to handle the dynamic and multi-layered risks present in 5G-enabled IoT environments. To address this issue, this research proposes a comprehensive hybrid cybersecurity framework specifically designed for smart cities.

The proposed framework combines three key technologies:

1) Machine Learning for intelligent anomaly detection and real-time threat identification.
2) Blockchain technology to ensure secure data transmission, authentication, and data integrity.
3) A multi-layered honeypot system to proactively collect threat intelligence and analyze attacker behaviour.

Overall, this research aims to contribute toward building a secure, resilient and trustworthy smart city ecosystem by integrating advanced technologies.

Keywords

Smart Cities, IoT, 5G, Cyber security, Threat Detection, Threat Mitigation, Machine Learning, Block chain, Honey pots, Network Security.

Introduction

Smart cities are becoming real because of IoT devices and 5G networks. IoT devices include smart cameras, sensors, and meters that collect and share data. With the help of 5G, these devices can communicate very fast. This helps cities improve traffic control, energy systems, healthcare services, and public safety.

However, this strong connection between devices also creates security problems. When many devices are connected, hackers get more chances to attack the system. Traditional security methods are not strong enough to protect such large and complex networks.

Background / Related Work

The cybersecurity situation in smart cities is an important research topic. Smart cities use IoT devices, 5G networks, and different urban systems together. Because of this combination, the system becomes more complex. Researchers study this area to understand both the benefits and the serious security problems that come with it.2.1. IoT in Smart Cities: A Double-Edged Sword

IoT devices form the bedrock of smart cities, enabling real-time data collection and automated control across diverse domains such as smart homes, smart cities, wearables, and connected cars [1]. This pervasive sensing and actuation capability, while driving efficiency, also introduces significant vulnerabilities. Uddin et al. emphasize that the rapid growth of IoT creates new avenues for cybercriminals, necessitating robust security measures. The heterogeneity of IoT devices, often characterized by limited computational resources, diverse communication protocols, and fragmented security standards, complicates the implementation of uniform protection mechanisms [2]. Attacks such as surveillance abuse, unauthorized access, and the financial costs associated with resolving security breaches are prominent concerns [3,4].

Andrade et al. [5] further underscore that IoT cybersecurity aspects represent a significant limitation in smart city development. They categorize IoT vulnerabilities based on OWASP IoT Top Ten attacks, identifying issues like weak passwords, insecure network services, lack of secure update mechanisms, and insufficient privacy protection. The interaction of IoT with cloud solutions, while enhancing data analytics and decision-making, expands the attack surface, introducing risks related to misconfigurations, metadata manipulation, and replay attacks [6].

The 5G Imperative and its Security Implications

The advent of 5G networks is a critical enabler for smart cities, promising ultra-fast transmission rates, extremely low latency, and massive device connectivity [7], [8]. This enhanced connectivity is vital for real-time applications like autonomous vehicles and critical infrastructure management. However, 5G also introduces a new layer of cybersecurity risks. Smys et al. and Serrano point out that the expanded network access and enhanced connectivity intrinsically increase cybersecurity risks, providing attackers with additional digital targets. The sharing of access channel infrastructure between mobile and wireless networks further complicates security.

Mohawesh et al. [9] provide a comprehensive overview of cybersecurity in 5G-enabled IoT networks, highlighting the need for ongoing work to mitigate weaknesses. They categorize 5G security challenges into user plane security, signaling storms, secure roaming, blockchain security, DoS attacks, compatibility strain, IoT device security, encryption vulnerabilities, NFV security issues, and layered network threats. The integration of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) in 5G, while offering flexibility, also centralizes control, making the SDN controller a single point of failure and an attractive target for attackers [10][11].

Emerging Cyber security Solutions

The academic community has responded to these challenges with a variety of innovative solutions:

- **Blockchain and Neural Networks:** Serrano and Smys et al. propose the Blockchain Random Neural Network for cybersecurity applications in smart cities. This approach leverages cryptographic concepts to secure user identity and data, with neural weights codifying user information. The decentralized nature of blockchain, combined with the learning capabilities of neural networks, aims to enhance authentication and resilience against breaches.
- **AI/ML for Threat Detection:** Deep learning techniques are increasingly being applied to detect network anomalies and cyberthreats in 5G networks [12] [13]. Ragab et al. introduce an Advanced Artificial Intelligence with a Federated Learning Framework for Privacy-Preserving Cyberthreat Detection (AAIFLF-PPCD) for IoT-assisted smart cities. This model uses Harris Hawk Optimization (HHO) for feature selection, a Stacked Sparse Auto-Encoder (SSAE) for cyberthreat detection, and the Walrus Optimization Algorithm (WOA) for hyperparameter tuning, demonstrating high accuracy in identifying various attacks.
- **Honey pots for Proactive Defense:** Ashraf et al. propose the Cybersecurity Threat Detection and Mitigation Framework for Smart Cities (CTDMF-SC), which utilizes a multi-tiered honeypot system for proactive threat detection[14]. Honeypots act as decoys, luring attackers and collecting intelligence on their tactics before they can reach critical infrastructure. This approach moves beyond reactive defense by actively engaging with threats[15].

Gaps in Existing Approaches

Despite these advancements, several critical gaps persist:

- **Integration and Orchestration:** Many proposed solutions tend to be specialized, focusing on a single aspect (e.g., detection, authentication) or a specific technology (e.g., blockchain, ML). A holistic framework that seamlessly integrates these diverse approaches into a cohesive, adaptive, and resilient system for smart cities is often lacking[16].
- **Real-world Applicability and Scalability:** While theoretical models and simulations demonstrate promise, the practical implementation and scalability of complex cybersecurity frameworks in the highly dynamic and resource-constrained environment of a real smart city remain significant challenges [17].
- **Proactive Threat Intelligence:** The emphasis often remains on detection and response. A more robust proactive stance requires continuous, real-time threat intelligence gathering and analysis to anticipate emerging attack vectors.
- **Human-Centric Security:** While technical solutions are crucial, the human element, including policy-making, user awareness, and incident response protocols, needs to be more deeply integrated into comprehensive frameworks [18].

Our proposed framework aims to bridge these gaps by offering an integrated, multi-layered approach that combines the strengths of advanced machine learning, blockchain, and honeypot technologies, specifically designed for the unique demands of 5G-enabled IoT smart cities.

Proposed Hybrid Cybersecurity Framework (HCF-5G-IoT)

The proposed Hybrid Cybersecurity Framework (HCF-5G-IoT) for smart cities is designed to

address the multifaceted and evolving threat landscape inherent in 5G-enabled IoT environments. This framework integrates three core pillars: intelligent threat detection via advanced machine learning, secure data provenance and authentication using blockchain, and proactive threat intelligence gathering through a multi-tiered honeypot system[19]. The synergistic combination of these elements aims to create a robust, adaptive, and resilient security posture for smart urban infrastructures.

Architectural Overview

The HCF-5G-IoT operates across several interconnected layers, as depicted in Figure 1.

Figure 1: Proposed Hybrid Cybersecurity Framework (HCF-5G-IoT) Architecture

```
graph TD
    subgraph Smart City Environment
        A[IoT Devices (Sensors, Actuators)] --> B(5G Network Infrastructure)
        B --> C(Smart City Applications & Services)
        C --> D(Critical Infrastructure: Energy, Transport, Water)
    end

    subgraph Cybersecurity Framework
        E[Multi-tiered Honeypot System] --> F(Threat Intelligence & Analysis Module)
        F --> G(Machine Learning-based Anomaly Detection Engine)
        G --> H(Security Orchestration & Automated Response - SOAR)
        H --> I(Blockchain-based Secure Authentication & Data Provenance)
        I --> C
        G --> C
        F --> G
        E --> G
        E --> H
        H --> D
        H --> B
        H --> A
    end
    style A fill:#f9f,stroke:#333,stroke-width:2px
    style B fill:#bbf,stroke:#333,stroke-width:2px
    style C fill:#ccf,stroke:#333,stroke-width:2px
    style D fill:#fcc,stroke:#333,stroke-width:2px
    style E fill:#afa,stroke:#333,stroke-width:2px
    style F fill:#add,stroke:#333,stroke-width:2px
    style G fill:#ddf,stroke:#333,stroke-width:2px
    style H fill:#fdf,stroke:#333,stroke-width:2px
    style I fill:#ffd,stroke:#333,stroke-width:2px
```

Explanation of Architectural Components:

Smart City Environment: This represents the operational domain, encompassing a vast array of IoT devices (sensors, actuators, connected vehicles), the underlying 5G network infrastructure providing high-speed, low-latency connectivity, and various smart city applications and services (e.g., smart traffic, smart grids, public safety)[20]. Crucially, this layer also includes critical infrastructure systems whose uninterrupted operation is vital for urban functioning.

- **Multi-tiered Honeypot System:** This component consists of strategically deployed decoy systems designed to mimic legitimate IoT devices, network services, and critical infrastructure elements. These honeypots are distributed across different network segments (perimeter, internal, specialized for OT/IoT protocols) to attract, engage, and analyze malicious activities without compromising real systems. They serve as early warning systems and a rich source of real-time threat intelligence[21][22].
- **Threat Intelligence & Analysis Module:** This module collects, aggregates, and processes data from the honeypot system, external threat feeds, and internal network logs[23]. It performs deep analysis to identify attack patterns, TTPs (Tactics, Techniques, and Procedures) of adversaries, and emerging vulnerabilities specific to the smart city context. This intelligence is then fed into other components for proactive defense.
- **Machine Learning-based Anomaly Detection Engine:** Leveraging the threat intelligence and real-time data streams from IoT devices and the 5G network, this engine employs advanced ML algorithms (e.g., deep learning, federated learning) to identify deviations from normal behaviour[24][25][26]. It is trained on both benign and known malicious patterns, continuously adapting to new threats. Its primary role is to detect sophisticated, zero-day attacks that might bypass signature-based defenses.
- **Blockchain-based Secure Authentication & Data Provenance:** This layer provides a decentralized, immutable ledger for managing identities, access controls, and data integrity across the smart city. It ensures secure authentication of IoT devices and users, tracks data origin and modifications, and establishes trust in data exchanges. This mitigates risks associated with identity spoofing, data tampering, and unauthorized access.

- **Security Orchestration & Automated Response (SOAR):** This central command and control unit orchestrates the overall cyber security response[27]. It receives alerts from the anomaly detection engine and threat intelligence module, automates predefined mitigation actions (e.g., isolating compromised devices, updating firewall rules, reconfiguring network slices), and facilitates human intervention for complex incidents. SOAR ensures rapid, consistent, and scalable responses to cyber incidents.

Operational Mechanisms and Interplay

The HCF-5G-IoT operates through a continuous feedback loop, where each component reinforces the others:

1. **Proactive Threat Intelligence:** The **Multi-tiered Honeypot System** actively engages with potential attackers, collecting detailed information on their methods. This raw data is then processed by the **Threat Intelligence & Analysis Module**, generating actionable insights into emerging threats.
2. **Intelligent Anomaly Detection:** The refined threat intelligence, combined with real-time network traffic and IoT device telemetry, feeds the **Machine Learning-based Anomaly Detection Engine**. This engine continuously monitors the 5G network and IoT ecosystem for anomalous behaviors that indicate a potential attack, including those not previously observed.
3. **Secure Foundation:** The **Blockchain-based Secure Authentication & Data Provenance** layer underpins the entire system by ensuring that all devices, users, and data interactions are authenticated, authorized, and recorded immutably[28]. This prevents foundational compromises and provides an auditable trail for forensic analysis.
4. **Automated and Orchestrated Response:** Upon detection of a threat or anomaly, the **SOAR** platform is activated. It leverages the intelligence from the analysis module and the detection engine to trigger automated mitigation actions. These actions can range from isolating a suspicious IoT device or reconfiguring a 5G network slice to updating security policies across the smart city infrastructure.
5. **Adaptive Learning:** The outcomes of mitigation actions and forensic analyses are fed back into the **Threat Intelligence & Analysis Module** and the **Machine Learning-based Anomaly Detection Engine**. This continuous learning process allows the framework to adapt to new attack vectors, refine its detection capabilities, and improve the effectiveness of its automated responses.

Addressing Key Challenges

This integrated approach directly tackles the specific cybersecurity challenges of 5G-enabled IoT smart cities:

- **Device Heterogeneity:** By leveraging ML for anomaly detection, the framework can learn the unique behavioral profiles of diverse IoT devices, identifying deviations regardless of their underlying architecture or protocols. Blockchain provides a unified, secure identity management system for all connected entities.
- **Real-time Operational Demands:** The 5G network's low latency is exploited by the ML engine for near real-time threat detection and by SOAR for rapid, automated responses, minimizing disruption to critical services.
- **Expanded Attack Surface:** The multi-tiered honeypot system proactively maps and understands the expanded attack surface, providing early warnings and intelligence on how attackers might exploit new vulnerabilities introduced by 5G and IoT proliferation.
- **Data Integrity and Trust:** Blockchain ensures the integrity and trustworthiness of critical data, preventing manipulation and providing verifiable records for all transactions and events within the smart city.
- **Proactive vs. Reactive:** The framework shifts the paradigm from reactive incident response to proactive threat anticipation and automated mitigation, significantly reducing the window of vulnerability.

By weaving these advanced technologies into a cohesive framework, HCF-5G-IoT aims to establish a resilient and intelligent defense mechanism capable of safeguarding the complex, dynamic, and critical infrastructure of future smart cities.

Results / Discussion

The efficacy of the proposed Hybrid Cybersecurity Framework (HCF-5G-IoT) is best understood through its potential impact on key performance indicators and its ability to address the inherent vulnerabilities of smart city ecosystems. While a full-scale empirical validation of such a comprehensive framework is a monumental undertaking, we can discuss its anticipated results and implications based on the strengths of its

constituent technologies and comparisons with existing approaches.

Enhanced Threat Detection Accuracy and Speed

The integration of a **Machine Learning-based Anomaly Detection Engine** with a **Threat Intelligence & Analysis Module** fed by **Multi-tiered Honeypots** is expected to significantly improve both the accuracy and speed of threat detection.

- **Superior Anomaly Detection:** Unlike signature-based intrusion detection systems that rely on known attack patterns, ML models, particularly deep learning architectures, can identify subtle deviations from normal behavior. This is crucial for detecting zero-day attacks and sophisticated, stealthy threats that are characteristic of advanced persistent threats (APTs) targeting critical infrastructure[29]. The AAIFLF-PPCD model discussed by Ragab et al. [7], for instance, achieved a 99.47% accuracy in cyberthreat detection using HHO, SSAE, and WOA, demonstrating the potential of such ML techniques.
- **Proactive Threat Identification:** The honeypot system acts as a sensor network for malicious activity. By luring attackers into controlled environments, it provides invaluable, real-time intelligence on new attack vectors, tools, and tactics. This proactive intelligence allows the ML models to be continuously retrained and updated, enabling the framework to anticipate threats rather than merely react to them. Ashraf et al. [8] highlight how honeypots can detect reconnaissance and vulnerability scanning, feeding predictive threat mitigation systems.
- **Reduced False Positives/Negatives:** The combination of diverse data sources (honeypots, network traffic, device logs) and advanced ML algorithms, coupled with human-in-the-loop validation facilitated by the SOAR platform, can lead to a substantial reduction in both false positives (benign activities flagged as malicious) and false negatives (actual attacks missed). This is a critical factor for operational efficiency in smart cities, where excessive false alarms can lead to alert fatigue and wasted resources.

Robust Authentication and Data Integrity

The **Blockchain-based Secure Authentication & Data Provenance** layer introduces a paradigm shift in trust management within smart cities.

- **Decentralized Identity Management:** Traditional centralized authentication systems present single points of failure. Blockchain offers a decentralized, tamper-proof mechanism for managing the identities of millions of IoT devices and users. This ensures that only authenticated entities can access network resources, mitigating risks like device cloning and identity spoofing, which are significant in 5G-IoT environments [3].
- **Immutable Data Records:** Every data transaction and event recorded on the blockchain is cryptographically secured and immutable. This provides an undeniable audit trail for data provenance, ensuring the integrity of critical information used for urban management and decision-making. In scenarios where data tampering could lead to physical harm (e.g., smart grids, traffic control), this immutability is paramount[29].
- **Enhanced Trust:** The transparency and verifiability offered by blockchain foster greater trust among diverse stakeholders in the smart city ecosystem, from citizens to service providers.

Automated and Adaptive Response Capabilities

The **Security Orchestration & Automated Response (SOAR)** platform is central to the framework's ability to provide rapid and scalable mitigation.

- **Rapid Incident Response:** By automating routine security tasks and orchestrating complex responses, SOAR drastically reduces the mean time to detect (MTTD) and mean time to respond (MTTR) to cyber incidents. This is particularly vital in 5G-enabled environments where the speed of attack propagation can be extremely high. Ashraf et al. [8] demonstrated a threat response time of 15 minutes with their CTDMF-SC framework.
- **Context-Aware Mitigation:** The SOAR platform, informed by real-time threat intelligence and ML-driven anomaly detection, can implement context-aware mitigation strategies. For instance, it can dynamically reconfigure 5G network slices, isolate compromised IoT devices, or update firewall rules based on the specific nature and severity of an attack[3].
- **Resource Optimization:** Automation frees up human security analysts to focus on more complex strategic tasks, optimizing resource allocation and improving overall security posture without requiring a proportional increase in human capital.

Future Work

Future research will focus on several key areas to further enhance and validate the HCF-5G-IoT framework:

1. **Empirical Validation and Scalability Testing:** Implementing a prototype of the HCF-5G-IoT in a controlled smart city testbed environment to gather empirical data on its effectiveness. This includes rigorous testing of the ML models' performance against diverse attack scenarios, evaluating the latency and throughput of the blockchain layer under high transaction loads, and assessing the realism and effectiveness of the honeypot deployments. Scalability studies will be crucial to understand the framework's performance as the number of IoT devices and 5G network traffic increases.
2. **Integration with Edge Computing and Network Slicing:** Investigating how the framework can optimally leverage edge computing resources for localized threat detection and mitigation, reducing reliance on centralized cloud infrastructure and minimizing latency. Furthermore, exploring the dynamic allocation of 5G network slices to create isolated, secure environments for critical smart city services, with the SOAR platform dynamically managing slice configurations in response to threats.
3. **Explainable AI (XAI) for Cybersecurity:** Developing XAI techniques within the ML-based anomaly detection engine to provide human-understandable explanations for detected threats. This will enhance trust in automated systems, facilitate faster decision-making by human analysts, and aid in forensic investigations.
4. **Policy and Governance Integration:** Researching the development of comprehensive policy frameworks and regulatory guidelines that align with the technical capabilities of HCF-5G-IoT. This includes addressing data privacy concerns (e.g., GDPR compliance), establishing clear roles and responsibilities for cybersecurity management across different city departments and private entities, and defining legal frameworks for automated response actions.
5. **Human-in-the-Loop Optimization:** Refining the interaction between automated SOAR responses and human security analysts. This involves designing intuitive interfaces for incident management, developing effective alert prioritization mechanisms, and optimizing workflows for human oversight and intervention in complex or high-stakes situations.
6. **Quantum-Resistant Cryptography Integration:** As quantum computing advances, current cryptographic standards may become vulnerable. Future work will explore integrating quantum-resistant cryptographic algorithms into the blockchain and secure communication protocols of the HCF-5G-IoT to ensure long-term security.
7. **Economic Impact and Cost-Benefit Analysis:** Conducting detailed economic analyses to quantify the cost-effectiveness of implementing HCF-5G-IoT, including the return on investment from preventing cyberattacks, reducing downtime, and improving public trust.

By pursuing these avenues, the HCF-5G-IoT can evolve into a truly resilient, intelligent, and practical cybersecurity solution, ensuring that smart cities can realize their full potential securely and sustainably.

Conclusion

The integration of IoT and 5G technologies in smart cities presents a complex security landscape. The benefits of enhanced connectivity and data-driven decision-making are undeniable, yet they come with inherent cyber security costs. The proposed HCF-5G-IoT framework, by integrating machine learning for anomaly detection, block chain for secure data provenance, and honey pots for proactive threat intelligence, offers a robust and adaptive defence mechanism. This multi-layered approach addresses the limitations of traditional, reactive security models by fostering a proactive, intelligent, and resilient cybersecurity posture. The framework's ability to learn from evolving threats, ensure data integrity, and automate rapid responses is crucial for maintaining the safety, privacy, and operational continuity of critical urban services.

References

[1] H. Uddin, M. Gibson, G. A. Safdar, T. Kalsoom, N. Ramzan, M. Ur-Rehman, and M. A. Imran, "IoT for 5G/B5G Applications in Smart Homes, Smart Cities, Wearables and Connected Cars," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Limassol, Cyprus, 2019, pp. 1–6.

[2] S. Smys, H. Wang, and A. Basar, "5G Network Simulation in Smart Cities using Neural Network Algorithm," *Journal of Artificial Intelligence and Capsule Networks*, vol. 3, no. 1, pp. 43–52, 2021.

[3] W. Serrano, "The Blockchain Random Neural Network for cybersecure IoT and 5G infrastructure in Smart Cities," in *Smart Cities and the Blockchain*, Springer, Cham, 2020, pp. 1–20.

[4] A. Akhunzada, S. ul Islam, and S. Zeadally, "Securing Cyberspace of Future Smart Cities," *IEEE Network*, vol. 33, no. 5, pp. 14–21, 2019.

[5] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," *IEEE Access*, vol. 8, pp. 228809–228831, 2020.

[6] V. Bhardwaj, A. Anooja, L. S. Vermani, S. Sunita, and B. K. Dhaliwal, "Smart cities and the IoT: an in-depth analysis of global research trends and future directions," *Discover Internet of Things*, vol. 4, no. 1, p. 19, 2024.

[7] M. Ragab, E. B. Ashary, B. M. Alghamdi, R. Aboalela, N. Alsaadi, L. A. Maghrabi, and K. H. Allehaibi, "Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities," *Scientific Reports*, vol. 15, no. 1, p. 4470, 2025.

[8] S. Ashraf, C. Choi, and A. Bilal, "CTDMF-SC: cybersecurity threat detection and mitigation framework for smart cities," *Journal of Cloud Computing*, vol. 13, no. 1, p. 12, 2026.

[9] R. Mohawesh, A. Al-yousef, T. Daradkeh, N. A. Alawad, M. A. Al-Shannaq, A. A. Saifan, R. Hammad, Y. N. Alahmad, and S. Maqsood, "Cybersecurity challenges and solutions in 5G-enabled internet of things," *Journal of Cloud Computing*, vol. 13, no. 1, p. 26, 2026.

[10] Pratik Narendra Gulhane, Aditi Rajesh Nimodiya ," A Review Paper on Cloud Computing" International Advanced Research Journal in Science, Engineering and Technology,Vol. 9, Issue 2, February 2022, DOI: 10.17148/IARJSET.2022.9212
ISSN (O) 2393-8021, ISSN (P) 2394-1588.

[11] Ahmad Jamy Kohistani, Mohammad Nawab Turan*, Nasrullah Rahimi, "Securing Digital Transformation in Community Services: AI-Based Solutions for Public Sector Cyber security" Applied Community Services Journal, Vol. 01, No. 02 (2025), p. 52-64, DOI: https://doi.org/10.61987/acsj.v1i2.1242.

[12] Ms. Tvisha Bhatia, "Cyber security Challenges in the Era of AI", International Journal for Multidisciplinary Research (IJFMR), E-ISSN: 2582-2160, International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com
IJFMR250664818 Volume 7, Issue 6, November-December 2025.

[13]Amisha Sharma, Dhairya Verma, Neha Sharma, Neeru Jindal, "A Review of Cyber Security and its Approaches with Recent Progress and Challenges", International Journal of Engineering Technology and Management Sciences, Issue: 6 Volume No.7 November - December – 2023, DOI:10.46647/ijetms.2023.v07i06.029 ISSN: 2581-4621.

[14] Bruce Middleton. "A history of cyber security attacks: 1980 to present." CRC Press, 2017.

[15] Saloni Khurana, "Review paper on cyber security." Int. J. Eng. Res. Technol. (IJERT) ISSN: 2278-0181, 2017.https://www.ijert.org/a-review-paper-on-cyber-security

[16] Ashwini Sheth, Sachin Bhosale, and Adnan Bukhari. "A Survey on Cyber
Security." Contemporary Research in India, Special Issue, 2021.

[17] Muqbil, Cyber security experts warn massive threat activity against SVB following collapse,ETCIO, 2023

[18] Alex Andrew, Sam Spillard, Joshua Collyer, and Neil Dhir. "Developing optimal causal cyber-defence agents via cyber security simulation." arXiv preprint arXiv:2207.12355,
2022.,https://doi.org/10.48550/arXiv.2207.12355

[19] Shah Md Istiaque, Md Toki Tahmid, Asif Iqbal Khan, Zaber Al Hassan, and Sajjad Waheed.,"State-of-the-Art Artificial Intelligence Based Cyber Defense Model." In 2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 1-6. IEEE, 2021.

[20] Gautam Srivastava, Rutvij H. Jhaveri, Sweta Bhattacharya, Sharnil Pandya, Praveen Kumar Reddy Maddikunta, Gokul Yenduri, Jon G. Hall, Mamoun Alazab, and Thippa Reddy Gadekallu. "XAI for cybersecurity: state of the art, challenges, open issues and future directions." arXiv preprint arXiv:2206.03585, 2022.

[21] IANS, 83% organisations in India reported rise in phishing attacks during Covid, ETCIO.com
From the Economic Times, September 2021

[22] Chuyi, Yan, Chen Zhang, Zhigang Lu, Zehui Wang, Yuling Liu, and Baoxu Liu. "Blockchain abnormal behavior awareness methods: a survey." Cybersecurity 5, no. 1: 5, 2022.

[23] Victor Mayoral-Vilches, Ruffin White, Gianluca Caiazza, and Mikael Arguedas. "Sros2: Usable cyber security tools for ros 2." In 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 11253-11259. IEEE, 2022.

[24]. Ricardo M. Czekster, Roberto Metere, and Charles Morisset. "Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings." Applied Sciences 12, no. 10 (2022): 5005.https://doi.org/10.3390/app12105005, 2022

[25] Carsten Maple, Matthew Bradbury, Anh Tuan Le, and Kevin Ghirardello. "A connected and autonomous vehicle reference architecture for attack surface analysis." Applied Sciences 9, no. 23:5101, 2019.

[26 13. Rahul K. Vigneswaran, R. Vinayakumar, K. P. Soman, and Prabaharan Poornachandran. security." In 2018 9th International conference on computing, communication and networking technologies (ICCCNT), pp. 1-6. IEEE, 2018.

[27]. Yuqi Chen, Bohan Xuan, Christopher M. Poskitt, Jun Sun, and Fan Zhang. "Active fuzzing for testing and securing cyber-physical systems." In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 14-26, 2020.

[28] Elhaam Abdulrahman Debas, Razan Sulaiman Alajlan, and MM Hafizur Rahman. "Biometric in Cyber Security: A Mini Review." In 2023 International

Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 570-574. IEEE, 2023.
[29] Mohammad Kamrul Hasan, AKM Ahasan Habib, Zarina Shukur, Fazil Ibrahim, Shayla Islam, and Md Abdur Razzaque. "Review on cyber-physical and cyber-security system in smart grid: Standards,protocols, constraints, and recommendations." Journal of Network and Computer Applications 209: 103540, 2023.
[30] Aušrius Juozapavičius, , Agnė Brilingaitė, Linas Bukauskas, and Ricardo Gregorio Lugo. "Ageand gender impact on password hygiene." Applied Sciences 12, no. 2: 894, 2022.,https://doi.org/10.3390/app12020894.