International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Mathematical Tools for Cyber security in Engineering Systems: A Review of Recent Trends and Applications

Dr. Anushka A. Patil [1], Dr. Ashok S Kulkarni [2] , Mr. Ashitosh P. Patil [3]
1 (Department of Mathematics,
PadamabhooshanVasntraodada Patil Institute of TechnologySangli, Maharashtra, India,
2 (Department of Mathematics,
D. A. B. N. Arts and Science College Chikhali, Sangli, India, Maharashtra,
3 (Department of Mechanical,
Bharati Vidyapeeth's College of Engineering, Kolhapur,Maharashtra, India)

Abstract - This paper presents a comprehensive review of the recent trends and applications of mathematical tools in enhancing the cybersecurity of engineering systems. The increasing interconnectedness and complexity of industrial control systems (ICS), operational technology (OT), cyber-physical systems (CPS), and the Internet of Things (IoT) in engineering have amplified their vulnerability to cyber threats. This review explores the crucial role of mathematical frameworks from cryptography, coding theory, formal methods, network science, and game theory in addressing these challenges. We examine the underlying mathematical principles of key techniques within these areas and analyse their application in securing engineering communication, data integrity, system verification, network resilience, and strategic defence. Furthermore, this paper identifies current research challenges and highlights potential future directions for leveraging mathematical advancements to fortify the cybersecurity posture of critical engineering infrastructure.

Keywords: Cybersecurity, Engineering Systems, Mathematical Tools, Cryptography, Coding Theory, Formal Methods, Network Science, Game Theory.

I. INTRODUCTION

The rapid growth of digital technologies has greatly transformed engineering systems, making industrial processes more automated, efficient, and connected. However, this progress has also introduced serious cybersecurity challenges. Modern engineering systems such as Industrial Control Systems (ICS), Operational Technology (OT), Cyber-Physical Systems (CPS), and the Internet of Things (IoT) are now highly interconnected and complex. While this connectivity improves performance, it also increases their exposure to cyber threats.

These systems play a crucial role in essential sectors like energy, manufacturing, transportation, and water management. Traditionally, they were designed with a focus on reliability and safety, with little attention to cybersecurity. As a result, many of these systems lack strong security features, making them vulnerable to cyberattacks. The impact of such attacks can be severe, including power outages, disruption of supply chains, environmental damage, and even risks to human life [9].

Engineering systems also differ from traditional IT systems in several ways. They operate in real time, interact directly with physical processes, and often rely on older (legacy) technologies that may have security weaknesses. Additionally, their wide geographical distribution and use of wireless communication create more opportunities for cyberattacks.

Because of these unique characteristics, traditional IT security methods are not sufficient to protect engineering systems. A more advanced and structured approach is needed—one that considers both cyber and physical aspects of these systems. Mathematical tools provide a strong and precise foundation for understanding and improving cybersecurity in this context.

This paper presents a comprehensive review of how mathematical methods can be used to enhance cybersecurity in engineering systems. It focuses on key areas such as cryptography, coding theory, formal methods, network science, and game theory. These tools help in securing communication, ensuring data integrity, verifying system safety, improving network strength, and developing effective defence strategies. The paper also discusses current challenges and future research directions, emphasizing the importance of mathematics in building secure and reliable engineering systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

II. MATHEMATICAL FOUNDATIONS OF CYBERSECURITY IN ENGINEERING SYSTEMS

Modern cybersecurity in engineering systems is grounded in several core mathematical disciplines that enable the design of secure and resilient infrastructures.

Number theory underpins cryptographic algorithms used for secure communication and authentication. Public-key systems such as RSA rely on the computational hardness of prime factorization [1], while Elliptic Curve Cryptography (ECC) employs algebraic structures over finite fields to achieve strong security with smaller key sizes, making it suitable for resource-constrained devices.

Linear and abstract algebra play a critical role in symmetric encryption and coding theory. Algorithms such as the Advanced Encryption Standard (AES) use matrix operations over finite fields [2], while algebraic coding theory ensures reliable data transmission through error detection and correction.

Probability and statistics are essential for intrusion detection [3] and risk assessment. Techniques such as Bayesian inference and Hidden Markov Models (HMM) enable the identification of anomalous patterns and support adaptive, data-driven security mechanisms.

Information theory provides measures such as entropy and mutual information to evaluate uncertainty and information leakage. These concepts are fundamental in assessing cryptographic strength and designing secure communication protocols, particularly in high-assurance systems.[4]

Graph theory facilitates the modelling and analysis of engineering networks. By representing systems as nodes and edges, graph-based methods support vulnerability analysis, attack path identification, and resilience enhancement [4].

Game theory offers a framework for modelling adversarial interactions between attackers and defenders. Concepts such as Nash equilibrium and Stackelberg games enable optimal decision-making and resource allocation in dynamic and constrained environments.

Collectively, these mathematical tools form the analytical foundation of modern cybersecurity, supporting applications ranging from encryption and authentication to anomaly detection and system resilience.

The key mathematical areas underpinning cybersecurity in engineering systems include several interconnected disciplines. Cryptography and number theory ensure confidentiality, integrity, and authentication through techniques such as RSA and elliptic curve cryptography (ECC). Linear algebra and algebraic structures support symmetric encryption algorithms like AES and enable error-correcting codes using finite fields and matrix operations. Probability and statistics play a vital role in intrusion detection and risk modelling through Bayesian and Markov-based approaches, allowing the identification of anomalous system behaviour. Information theory contributes by quantifying uncertainty and potential data leakage using measures such as entropy. Graph theory is employed to model network structures, facilitating vulnerability assessment and attack path analysis. Additionally, game theory provides strategic frameworks for modelling attacker–defender interactions, enabling optimal decision-making and efficient resource allocation in cybersecurity systems.

III. EMERGING TRENDS IN MATHEMATICAL APPROACHES TO CYBERSECURITY

The field of cybersecurity in engineering systems is rapidly evolving due to emerging technologies, increasing threat sophistication, and the growing interconnectivity of devices. In response, recent research emphasizes the integration of advanced mathematical tools to develop resilient, adaptive, and future-proof security frameworks.

A major advancement is the development of **post-quantum cryptography (PQC)**. Classical cryptographic schemes such as RSA and elliptic curve cryptography are vulnerable to quantum attacks, particularly due to Shor's algorithm [6]. To address this, new cryptographic approaches based on hard mathematical problems have been proposed, including lattice-based, code-based, and multivariate polynomial cryptography. These approaches are currently being standardized and are expected to form the foundation of next-generation secure communication systems.

Another important trend is the adoption of **blockchain and distributed ledger technologies**. These systems use cryptographic hash functions, public-key encryption, and consensus mechanisms to provide decentralized and tamper-resistant security[5]. Their mathematical foundations include number theory, graph theory, and probability, making them suitable for applications in supply chains, smart grids, and industrial automation.

The integration of **artificial intelligence (AI) and machine learning (ML)** has significantly enhanced cybersecurity capabilities. These techniques rely on mathematical concepts such as linear algebra, optimization, probability, and statistics[7]. Machine learning

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

models, including support vector machines and neural networks, are widely used for intrusion detection, anomaly detection, and malware classification, enabling real-time and adaptive threat mitigation.

Formal methods and mathematical logic are increasingly used to ensure system correctness and security. Techniques such as model checking and theorem proving allow for the verification of system properties before deployment. These approaches are particularly critical in safety-sensitive engineering domains [8], where system failures can have severe consequences.

Additionally, **game theory** is being applied to model strategic interactions between attackers and defenders. By using concepts such as Nash equilibrium and Stackelberg games, these models support optimal decision-making and efficient allocation of limited cybersecurity resources.

Overall, these developments highlight a shift toward mathematically rigorous, proactive, and adaptive cybersecurity solutions. As engineering systems continue to grow in complexity and connectivity, such approaches will play a crucial role in ensuring their security and resilience.

The key emerging areas in cybersecurity for engineering systems reflect the growing need for advanced and mathematically robust solutions. Post-quantum cryptography addresses the limitations of classical cryptographic techniques in the presence of quantum computing by employing quantum-resistant approaches such as lattice-based and code-based cryptography, which are currently undergoing standardization. Blockchain and distributed ledger technologies provide decentralized and tamper-resistant security mechanisms through the use of cryptographic hashing, Merkle trees, and consensus algorithms, with significant applications in IoT and smart systems. Artificial intelligence and mathematical optimization further enhance cybersecurity by utilizing machine learning models based on optimization techniques and matrix operations for intrusion detection, anomaly identification, and real-time threat mitigation. Additionally, formal methods and verification techniques employ mathematical logic, model checking, and temporal logic to ensure system correctness and security, particularly in engineering control systems where reliability is critical.

IV. APPLICATIONS OF CRYPTOGRAPHY IN ENGINEERING SYSTEMS

Cryptography plays a vital role in ensuring the security, integrity, and reliability of modern engineering systems. Its applications span multiple domains, where it is integrated with mathematical modelling, control systems, and intelligent algorithms to address domain-specific security challenges.

A. Smart Grids

In smart grid systems, cryptography is used to secure communication between distributed components such as sensors, smart meters, and control centres. Mathematical optimization and graph theory are applied to model grid operations and detect vulnerabilities. Cryptographic protocols ensure data confidentiality and integrity, preventing unauthorized access and manipulation of grid data. **e.g.** A secure smart grid communication model employs encryption for data transmission between substations and control centres. Attack detection is enhanced using graph-based anomaly detection techniques, ensuring resilience against cyber-physical attacks [9].

B. Industrial Control Systems (ICS)

Industrial Control Systems, including SCADA systems, rely on cryptographic mechanisms to secure control signals and operational data. These systems combine deterministic control models with encryption to maintain system integrity. Intrusion detection systems (IDS) use probabilistic models and artificial intelligence to identify abnormal behaviour in real time [3].

e.g. In a manufacturing plant, encrypted communication between programmable logic controllers (PLCs) and supervisory systems prevents unauthorized command injection. Machine learning-based IDS detects deviations in control signals, reducing the risk of system compromise.

C. Autonomous Vehicles

Autonomous vehicles depend on secure communication and decision-making systems. Cryptography ensures secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Game theory and control system models are used to handle adversarial scenarios, while AI-based sensor fusion detects spoofing and tampering [4].

e.g. In intelligent transportation systems, encrypted V2V communication prevents malicious message injection. AI algorithms analyze sensor data (e.g., LiDAR, GPS) to detect inconsistencies caused by spoofing attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

D. Internet of Things (IoT) Devices

IoT systems operate in resource-constrained environments, requiring lightweight cryptographic techniques such as elliptic curve cryptography (ECC). Secure key distribution and graph-based trust models are used to ensure safe communication among devices in large-scale networks. e.g. In a smart home system, lightweight encryption secures communication between devices like sensors, cameras, and controllers. Trust-based models evaluate device behaviour to prevent compromised nodes from spreading malicious data [10].

Across these applications, cryptography works in conjunction with mathematical tools such as graph theory, probability, optimization, and artificial intelligence to provide multi-layered security. These integrated approaches enhance the resilience, adaptability, and reliability of engineering systems in the face of evolving cyber threats.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS:

Despite significant progress, several challenges persist in securing engineering systems. Key issues include scalability constraints in large-scale environments, difficulties in integrating modern security mechanisms with legacy systems, and the need for stronger interdisciplinary collaboration. The rapidly evolving threat landscape, including AI-driven attacks and advanced persistent threats, necessitates adaptive and robust mathematical models. Resource limitations in embedded devices further demand lightweight and efficient cryptographic solutions. Additional challenges include ensuring data privacy, achieving interoperability across heterogeneous systems, addressing risks in cyber-physical environments, and the lack of standardized benchmarking frameworks. Moreover, the emergence of quantum computing poses a serious threat to existing cryptographic techniques.

Future research should focus on developing scalable and energy-efficient security algorithms, advancing post-quantum cryptography, and integrating artificial intelligence with mathematical frameworks for proactive threat detection. Emphasis should also be placed on standardization, formal verification, real-world testing environments, and privacy-preserving mechanisms[6]. A multidisciplinary approach combining mathematics, engineering, and cybersecurity will be essential to address these challenges and ensure the resilience of next-generation engineering systems.

VI. CONCLUSION

Mathematical tools form the backbone of cybersecurity in engineering systems. This paper has reviewed fundamental and advanced mathematical approaches, their applications across engineering domains, and emerging directions such as post-quantum security and AI-enhanced detection. Future research must focus on scalable, adaptive, and integrated mathematical frameworks to address the growing complexity of cyber-physical threats.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.
[2] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” FIPS PUB 197, Nov. 2001, doi: 10.6028/NIST.FIPS.197.
[3] D. E. Denning, “An intrusion-detection model,” *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987, doi: 10.1109/TSE.1987.232894.
[4] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.
[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. https://doi.org/10.48550/arXiv.0807.1099
[6] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proc. 35th Annu. Symp. Foundations of Computer Science (FOCS)*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.
[7] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.
[8] E. M. Clarke, O. Grumberg, and D. A. Peled, *Model Checking*. Cambridge, MA, USA: MIT Press, 1999, doi: 10.7551/mitpress/4721.001.0001.
[9] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber–physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012, doi: 10.1109/JPROC.2011.2161428.
[10] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: Security protocols for sensor networks,” *Wireless Networks*, vol. 8, no. 5, pp. 521–534, Sep. 2002, doi: 10.1023/A:1016598314198.