IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

The Data Sentinel: Redefining Cybersecurity in the Big Data Epoch

Prof. Shegar S. R.[1] and Gadge Siddhesh Sunil[2]
Guide, Master of Computer Engineering, Samarth College of Engineering & Management, Belhe, India [1]
Student, Master of Computer Engineering, Samarth College of Engineering & Management, Belhe, India [2]

Abstract: *In the current digital landscape, data has emerged as the new oil—fueling innovation, governance, healthcare, and nearly every aspect of modern life. However, the exponential growth of data has also led to increasingly complex cybersecurity threats. Traditional security systems, built for static and limited data environments, are now overwhelmed by the dynamic, decentralized, and high-velocity nature of big data. This paper introduces the concept of the "Data Sentinel"—an advanced cybersecurity framework designed specifically to meet the unique challenges posed by the big data epoch. By leveraging artificial intelligence (AI), blockchain, real-time analytics, and behavioral insights, the Data Sentinel provides an adaptive, proactive, and intelligent defense mechanism against modern cyber threats. The study explores the technological foundation, applications across various sectors, and the potential challenges of implementing such a system*.

Keywords: Big Data, Cybersecurity, Data Sentinel, Artificial Intelligence, Real-time Analytics, Threat Detection

I. INTRODUCTION

As the digital age advances, data generation has reached unprecedented levels, driven by smartphones, IoT devices, social media platforms, and cloud services. While this explosion of data holds immense potential, it also exposes critical vulnerabilities in current cybersecurity models. Conventional cybersecurity infrastructures typically rely on perimeter-based protection, static rule sets, and manual threat detection processes. These methods are increasingly ineffective in environments where data moves at high speed, changes formats rapidly, and is shared across decentralized networks. To address these challenges, a paradigm shift is required—a model that not only detects threats but also predicts and neutralizes them in real time. The "Data Sentinel" emerges as a visionary approach that redefines the role of cybersecurity in a big data ecosystem. It embodies a set of intelligent, adaptive, and self-learning mechanisms capable of evolving alongside emerging threats.

II. RELATED WORK

In the field of cybersecurity, especially in the context of big data, several advancements have been made in an attempt to address the challenges posed by the dynamic, large-scale, and high-velocity nature of data. The Data Sentinel concept draws upon and extends ideas from various works in the field. Below are some notable contributions that align with or influence the development of the Data Sentinel framework.

1. AI and Machine Learning in Cybersecurity

Machine learning (ML) and artificial intelligence (AI) have been key components in transforming cybersecurity from static defense systems to more **adaptive and intelligent frameworks**. A number of researchers have focused on using **supervised learning** and **unsupervised learning** models to detect and mitigate anomalies in data streams.

DOI: 10.48175/IJARSCT-26172

- **Deep Learning for Intrusion Detection**: One significant development in this area is the use of **deep learning algorithms** for anomaly detection in large-scale systems. For example, some works have demonstrated the effectiveness of **convolutional neural networks (CNNs)** and **recurrent neural networks (RNNs)** in identifying unusual patterns that could indicate security breaches or attacks in real-time data.
- **Anomaly Detection in Big Data**: Researchers have developed algorithms that can analyze massive datasets (such as user activity logs, network traffic data, etc.) to identify outliers or anomalies. This work often includes techniques such as **clustering**, **decision trees**, and **ensemble methods** to improve detection accuracy and reduce false positives.

2. Blockchain for Cybersecurity

- Blockchain technology has been widely explored as a means of enhancing data security. **Blockchain-based security** systems leverage the inherent properties of blockchain—**decentralization, immutability, and transparency**—to prevent unauthorized access, tampering, and data manipulation.
- **Decentralized Access Control**: Some works have focused on using blockchain for **secure access management**. By storing access rights and permissions on the blockchain, these systems prevent unauthorized changes and offer traceable records of who accessed what data and when. **Smart contracts** on blockchain can automate access control decisions in a trustless environment.
- **Auditability and Data Integrity**: Blockchain has also been used for maintaining tamper-proof logs for **audit trails**. This work aligns with the **Data Sentinel** approach, which utilizes blockchain to create immutable logs of activities related to sensitive data, ensuring transparency and accountability.

3. Real-Time Analytics and Behavioral Insights

Several studies have investigated the use of **real-time data analytics** and **behavioral analytics** to enhance cybersecurity systems. These systems focus on tracking user behavior patterns and detecting anomalies that could indicate insider threats or unauthorized access.

- **Behavioral Biometrics**: Research has explored **behavioral biometrics** such as keystroke dynamics, mouse movements, and biometric authentication techniques to identify users and detect abnormal behavior. These methods focus on **monitoring behavioral patterns** over time to spot inconsistencies that could indicate compromised accounts or malicious insiders.
- **User and Entity Behavior Analytics (UEBA)**: UEBA solutions use machine learning to establish a **baseline of normal user behavior** and flag deviations from this baseline. By integrating **network traffic monitoring** with **AI algorithms**, these solutions are able to detect suspicious activities in near real-time.

4. Cybersecurity in Cloud Environments

The rapid growth of cloud computing has introduced new challenges in cybersecurity, as data is no longer confined to a single location or managed by one organization. Various studies have focused on securing **multi-cloud environments** and **hybrid clouds**, which are critical to the **Data Sentinel** approach.

- **Zero Trust Architecture (ZTA)**: ZTA is a security model that assumes **no user or device is trusted** by default, whether inside or outside the organization. Several research papers have discussed how ZTA can be integrated into cloud computing to provide continuous verification of user identities, devices, and data interactions.
- **Cloud-native Security Tools**: Research has also explored **cloud-native security tools** such as **container security** and **serverless computing** protections to secure data stored and processed in cloud infrastructures. These tools help ensure that cloud applications remain secure even as they scale and evolve.

DOI: 10.48175/IJARSCT-26172

5. Integration of Cybersecurity Frameworks

A growing body of work is focused on integrating various cybersecurity measures into a cohesive framework that can handle the scale and complexity of modern digital environments.

- **NIST Cybersecurity Framework**: The **National Institute of Standards and Technology (NIST)** framework is one of the most recognized cybersecurity frameworks in the industry. Several research works have suggested **customized adaptations of NIST** for big data environments, with a focus on **adaptive security policies**, threat modeling, and continuous monitoring.
- **Security Information and Event Management (SIEM)**: Many organizations are integrating **SIEM** solutions to detect and respond to security events in real-time. The integration of **big data analytics** with SIEM platforms is an area of ongoing research, where data from various sources (e.g., logs, sensors, network traffic) is processed and analyzed to detect threats across large datasets.

6. Challenges and Limitations in Existing Cybersecurity Approaches

While there have been significant advancements in each of these areas, challenges remain in their implementation and scalability in the big data context. Some of the ongoing issues are:

- **Data Privacy and Ethics**: The use of AI, machine learning, and behavioural analytics raises concerns about the ethical implications of constant surveillance and the potential violations of privacy laws.
- **Computational Demands**: Real-time processing of large datasets for anomaly detection and threat mitigation is computationally expensive and resource-intensive.
- **Interoperability with Legacy Systems**: The adoption of advanced cybersecurity technologies in organizations with legacy systems remains a significant hurdle.

III. FUNDAMENTAL CONCEPTS OF CYBER SECURITY, CYBER-ATTACKS, AND CYBER-SPACE THREATS

The Big Data Challenge in Cybersecurity

The big data environment is characterized by five core attributes: volume, velocity, variety, veracity, and value. Each of these dimensions introduces unique security challenges.

- **Volume** refers to the massive amounts of data generated every second, which creates a wider surface area for attacks. For instance, managing security across millions of data points simultaneously is beyond human capacity.
- **Velocity** denotes the rapid speed at which data is created and transmitted; this reduces the window for detecting and responding to threats.
- **Variety** encompasses the different types of data—from structured database entries to unstructured images, videos, and sensor readings—making it difficult to apply a one-size-fits-all security solution.
- **Veracity** highlights issues of data accuracy and integrity; tampered or false data can lead to misleading analytics and undetected breaches.

Lastly, **value** emphasizes that as data becomes more valuable, it attracts more sophisticated cybercriminals. In essence, big data environments demand security systems that are as dynamic and complex as the data itself.

Concept of the Data Sentinel

The Data Sentinel is a multi-layered cybersecurity framework that acts as a real-time guardian of digital ecosystems. Unlike traditional systems that focus on firewalls and antivirus software, the Data Sentinel integrates several advanced technologies to create a dynamic and intelligent defense model. First, it employs **AI-powered anomaly detection** to monitor and analyze real-time data streams. These algorithms can identify subtle deviations from normal behavior, such as a user accessing sensitive data outside of business hours. Second, **blockchain technology** is utilized for secure access control and tamper-proof data logs. Each action or transaction is recorded on a distributed ledger, ensuring transparency and making unauthorized changes virtually impossible. Third, **behavioral analytics** allow the system to study user patterns over time, which helps in identifying insider threats or compromised accounts. Lastly, the system supports **real-time policy adaptation**, where security rules automatically adjust based on detected threat levels. For example, if suspicious activity is detected on a user account, the system might escalate authentication requirements or temporarily block access. These components work together to create a responsive and intelligent cybersecurity infrastructure.

Technologies Empowering the Data Sentinel

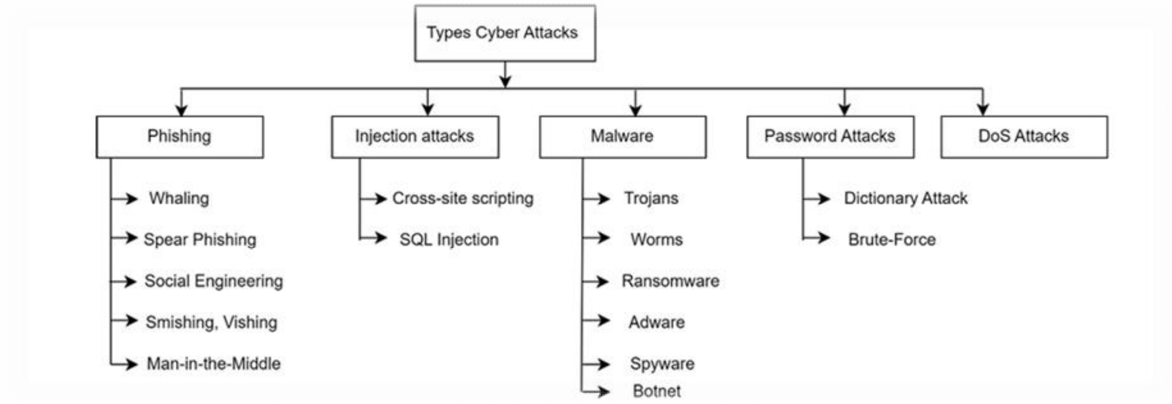
The successful implementation of the Data Sentinel model depends on a trio of cutting-edge technologies. Artificial Intelligence (AI) and Machine Learning (ML) play a foundational role in threat detection and response. These technologies can sift through enormous datasets to identify patterns, detect anomalies, and even predict future threats based on historical data. Unlike traditional rule-based systems, AI adapts and evolves, reducing false positives and improving detection accuracy. Secondly, blockchain introduces a decentralized approach to data security. By creating a distributed, immutable ledger, blockchain ensures that access logs, user permissions, and data transactions are transparent and secure. This drastically reduces the risk of insider tampering and makes auditing more efficient. Lastly, the rise of cloud-native security is critical in protecting data stored and processed in cloud environments. Concepts such as zero-trust architecture, container security, and continuous compliance ensure that security policies follow data across hybrid and multi-cloud systems. Together, these technologies form the backbone of the Data Sentinel and enable its adaptive capabilities**.**

Challenges and Limitations

Despite its strengths, the Data Sentinel framework faces several implementation challenges. One of the primary concerns is the computational demand of AI and real-time analytics. Processing and analyzing vast amounts of data in real-time requires significant infrastructure and energy resources. This makes adoption more difficult for small and mid-sized organizations. Additionally, the use of behavioral analytics and surveillance technologies raises ethical and privacy concerns. Employees and users may object to constant monitoring, and regulations such as the GDPR mandate strict consent and data usage policies. Another limitation is the integration of new technologies with legacy systems, especially in older organizations or government agencies that rely on outdated software. Transitioning to a Data Sentinel model involves both technological upgrades and cultural change—requiring investment in training, system redesign, and policy development. These limitations must be addressed through cross-sector collaboration and thoughtful regulation.

IV. TYPES OF CYBER ATTACKS

- **Untargeted Attacks:** In this type of attack, attackers do not have a specific target on the device, service, or user they are attacking. Phishing, water holing, ransomware, and scanning are some of the techniques used in these types of attacks.
- **Targeted Attacks:** Targeted attacks are explicitly aimed at specific organizations because of their particular interest in financial gain. These types of attacks can be more severe because they exploit vulnerabilities in target personnel or processes. For example, spear phishing botnets are deployed for DDOS and supply chain subversion.
- **Insider Threats:** This involves employees who launch malicious insider threat activities to breach security systems and steal sensitive information.
- **Cyberwarfare:** For economic or social reasons, governments commit cybercrimes against other countries, resulting in cyberwarfare.



V. CASE STUDIES

Healthcare: Ensuring the Security of Patient Data

- **Context**: Healthcare organizations manage vast amounts of sensitive data, including patient records, medical histories, test results, and real-time data from IoT devices used in patient monitoring. Securing this data is essential not only to ensure patient privacy but also to maintain trust and comply with regulations like **HIPAA (Health Insurance Portability and Accountability Act)**.

Application of the Data Sentinel:

- **AI-Powered Threat Detection**: An AI-powered anomaly detection system is used to continuously monitor access patterns to electronic health records (EHR). The system can identify unusual activity, such as a healthcare provider accessing patient records outside their normal scope of work or at unauthorized times (e.g., late-night logins). This real-time detection helps prevent unauthorized access or potential insider threats.
- **Blockchain for Data Integrity**: Blockchain technology is used to ensure that any changes made to medical records are securely logged and immutable. Every access, modification, or update to patient data is recorded on a distributed ledger, ensuring full transparency and preventing tampering.
- **Behavioral Analytics**: The system also tracks the behaviors of healthcare staff and devices. For example, if a nurse consistently accesses records only for their assigned patients, an unexpected login from a new location may trigger an alert. Additionally, a patient's monitoring devices, such as a heart rate monitor, are also constantly assessed for anomalies that could indicate compromised data or potential security breaches.

Financial Sector: Fraud Prevention and Transaction Security

- **Context**: The financial industry is a prime target for cybercriminals due to the high value of the data involved—bank account information, credit card data, investment records, and personal financial data. Fraud detection and transaction security are critical in maintaining customer trust and financial stability.

Application of the Data Sentinel:

- **Real-Time Transaction Monitoring**: AI algorithms analyze vast amounts of financial transaction data in real time to detect fraudulent activities. For instance, the system can identify abnormal transactions such as large withdrawals or transfers that deviate from a user's typical spending patterns. The AI also cross-references these patterns with external data sources (e.g., market trends or news) to determine whether a transaction might be linked to larger financial crimes like money laundering.

- **Blockchain for Identity Verification**: Blockchain is employed to create **secure digital identities** for users, ensuring that only authorized users can access sensitive financial systems. Using blockchain-based **identity verification** systems allows for faster and more secure **KYC (Know Your Customer)** processes, ensuring that fraudulent accounts or individuals cannot bypass traditional identity checks.
- **Behavioral Analytics for Insider Threats**: Financial institutions also employ behavioral analytics to detect **insider threats**. For example, if an employee attempts to access customer accounts they typically don't work with, or if an employee logs in at unusual hours, the system will raise an alert.

Outcome:

- **Reduced Fraud**: Real-time transaction monitoring enabled the bank to reduce fraud cases by 35%, as anomalous transactions were flagged and stopped before they could cause significant financial loss.
- **Improved Customer Trust**: The integration of blockchain for secure identity verification and AI for fraud detection helped strengthen customer confidence in the financial institution's security practices.

Outcome:

- **Increased Patient Privacy**: The integration of AI, blockchain, and behavioral analytics provides a highly secure and adaptive environment for managing patient data.
- **Compliance with Regulations**: The healthcare organization was able to meet HIPAA compliance requirements by ensuring all actions related to patient data were logged, secure, and transparent.

Government Sector: Securing National Data

- **Context**: Governments handle a wide range of sensitive data, from classified national security information to citizens' personal records. Ensuring that this data remains protected from both external and internal threats is crucial for national security and public trust.

Application of the Data Sentinel:

- **AI-Powered Threat Intelligence**: The government implemented an AI-driven security system that scans vast amounts of data from multiple sources (e.g., email communications, social media, network traffic) for potential threats or data breaches. By continuously monitoring this data, the system can detect signs of cyber espionage, unauthorized access, or data exfiltration, allowing immediate action to be taken.
- **Blockchain for Secure Data Sharing**: With many government agencies needing to exchange sensitive information, blockchain technology is utilized to **securely transfer data** between departments, agencies, or external contractors. Blockchain ensures that the data cannot be tampered with during transit and that all transactions are recorded on an immutable ledger.
- **Behavioral Analytics to Detect Insider Threats**: Insider threats—whether from malicious employees or compromised individuals—are a significant concern for government agencies. The **Data Sentinel's behavioral analytics** systems continuously monitor employee activity patterns, detecting anomalies such as unusual login times, file accesses, or email communications. These deviations trigger alerts that enable security teams to investigate the source of the threat.

Outcome:

- **Enhanced National Security**: The ability to detect and neutralize insider and external threats in real-time ensured that national security data remained secure.
- **Efficient Data Sharing**: Blockchain technology enabled secure and transparent data sharing between government agencies, reducing the risk of information leaks or unauthorized data access.

DOI: 10.48175/IJARSCT-26172

Retail Industry: Securing Customer Data and Payment Systems

- **Context**: Retail businesses, particularly e-commerce platforms, store sensitive customer information, including payment card details, addresses, and personal preferences. Securing this data is vital to prevent cyberattacks such as **data breaches** and **credit card fraud**.

Application of the Data Sentinel:

- **Real-Time Monitoring for Payment Fraud**: The e-commerce platform utilizes real-time data monitoring to detect suspicious activity in payment systems. Machine learning algorithms analyze purchasing behaviors and flag unusual transactions, such as a sudden change in purchasing frequency or high-value purchases from unfamiliar IP addresses.
- **Blockchain for Payment Security**: Blockchain-based **payment systems** are integrated to ensure that every transaction is encrypted and recorded on an immutable ledger, making it nearly impossible to alter transaction details post-purchase. This helps prevent fraud in digital transactions, ensuring transparency and accountability.
- **Behavioral Analytics for Customer Authentication**: Behavioral analytics helps verify that the person making the transaction matches the typical behavior of the legitimate customer. If there is an inconsistency, the system triggers additional authentication steps (e.g., two-factor authentication) before proceeding.

Outcome:

- **Prevention of Data Breaches**: The integration of real-time fraud detection, blockchain for payment security, and behavioral analytics significantly reduced the occurrence of data breaches and payment fraud.
- **Improved Customer Experience**: Customers were more confident in making transactions on the platform due to enhanced security measures, leading to increased trust and repeat business.

Telecommunications: Securing Customer Communication Networks

- **Context**: Telecom companies manage vast communication networks that carry sensitive information such as phone conversations, internet usage data, and private messages. Securing these networks from cyber threats is essential to maintaining service integrity and customer trust.

Application of the Data Sentinel:

- **AI-Powered Network Traffic Analysis**: Telecom companies employ AI systems that continuously analyze network traffic for signs of cyberattacks, such as **DDoS (Distributed Denial of Service) attacks**, **malware** injections, or attempts to access restricted areas of the network.
- **Blockchain for Secure Communications**: Blockchain technology is used to secure communication logs and ensure that call records and data packets cannot be tampered with. This enhances the privacy and integrity of both **voice** and **data communications**.
- **Real-Time Threat Detection**: AI-driven systems continuously monitor the network for abnormal patterns, such as a surge in data traffic or suspicious device connections, and can automatically isolate potentially compromised segments of the network to prevent further breaches.

Outcome:

- **Network Security Improvement**: The telecom company was able to significantly reduce **service disruptions** caused by cyberattacks, improving both operational uptime and customer satisfaction.
- **Enhanced Customer Privacy**: Blockchain integration ensured that customer communication data remained secure and immutable, providing customers with greater privacy assurance.

DOI: 10.48175/IJARSCT-26172

VI. CONCLUSION

In conclusion, the Data Sentinel represents a fundamental shift in how cybersecurity is conceptualized and implemented in the era of big data. It goes beyond traditional defense mechanisms to provide an intelligent, proactive, and adaptable framework capable of responding to the ever-evolving threat landscape. As data continues to grow in volume and value, the systems protecting it must become equally sophisticated. The integration of AI, blockchain, and behavioral analytics offers a robust solution to modern cybersecurity challenges. However, realizing the full potential of the Data Sentinel will require addressing computational, ethical, and infrastructural hurdles. If implemented thoughtfully, it promises not just to secure data but to **empower organizations with confidence in their digital operations**—turning cybersecurity from a barrier into an enabler of innovation.

REFERENCES

[1] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, 2020. DOI:10.1016/j.jnca.2020.102630.

[2] M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial IoT networks through a reliable cyber attack detection model," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6154–6162, 2020. DOI:10.1109/TII.2020.2970074.

[3] R. Mitchell and R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 16–30, 2015. DOI: 10.1109/TDSC.2014.2312327.

[4] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," IEEE Transactions on Dependable and Secure Computing, 2019, to be published. DOI:10.1109/TDSC.2019.2952332.

[5] M. S. Hossain, M. Al-Hammadi, and G. Muhammad, "Automatic fruit classification using deep learning for industrial applications," IEEE Transactions on Industrial Informatics, vol. 15, no. 2, pp. 1027–1034, 2019. DOI: 10.1109/TII.2018.2875149.

[6] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Systems, vol. 189, p. 105124, 2020. DOI: 10.1016/j.knosys.2019.105124.

[7] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," Applied Soft Computing, vol. 71, pp. 66–77, 2018. DOI: 10.1016/j.asoc.2018.06.017.

[8] G. E. Hinton, "A practical guide to training restricted boltzmann machines," in Neural networks: Tricks of the trade. Springer, 2012, pp. 599–619. [9] K. Liu, L. M. Zhang, and Y. W. Sun, "Deep boltzmann ma chines aided design based on genetic algorithms," Applied Me chanics & Materials, vol. 568-570, pp. 848–851, 2014. DOI: 10.4028/www.scientific.net/AMM.568-570.848.

[10] W. Deng, H. Liu, J. Xu, H. Zhao, and Y. Song, "An improved quantum inspired differential evolution algorithm for deep belief network," IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 10, pp. 7319–7327, 2020. DOI: 10.1109/TIM.2020.2983233.

[11] S. Boettcher and A. Percus, "Nature¨ s way of optimizing," Artificial Intelligence, vol. 119, no. 1-2, pp. 275–286, 2000. DOI: 10.1016/S0004 3702(00)00007-2.

[12] G. Q. Zeng, X. Q. Xie, M. R. Chen, and J. Weng, "Adaptive population extremal optimization-based pid neural network for multivariable non linear control systems," Swarm and Evolutionary Computation, vol. 44, pp. 320–334, 2019. DOI: 10.1016/j.swevo.2018.04.008.

[13] C. Zhang, P. Lim, A. K. Qin, and K. C. Tan, "Multiobjective deep belief networks ensemble for remaining useful life estimation in prognostics," IEEE Transactions on Neural Networks and Learning Systems, vol. 28, no. 10, pp. 2306–2318, 2017. DOI: 10.1109/TNNLS.2016.2582798.

[14] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6182–6191, 2020. DOI: 10.1109/TII.2020.2975227.

[15] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," IEEE Systems Journal, vol. 11, no. 3, pp. 1644–1652, 2017. DOI: 10.1109/JSYST.2014.2341597.

[16] D. Zheng, Z. Hong, N. Wang, and P. Chen, "An improved LDA-based ELM classification for intrusion detection algorithm in IoT application," Sensors, vol. 20, no. 6, p. 1706, 2020. DOI: 10.3390/s20061706.

[17] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018. DOI: 10.1109/ACCESS.2018.2836950.

[18] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," Neural computation, vol. 18, no. 7, pp. 1527–1554, 2006. DOI: 10.1162/neco.2006.18.7.1527.

[19] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mech anism," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2505–2516, 2017. DOI: 10.1109/TSG.2017.2703842.

[20] S. Manimurugan, S. Almutairi, A. Majed, Mohammed, C. Naveen, S. Ganesan, and P. Rizwan, "Effective attack detection in in ternet of medical things smart environment using a deep belief neural network," IEEE Access, vol. 8, pp. 77396–77404, 2020. DOI:10.1109/ACCESS.2020.2986013.

[21] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," IEEE Access, vol. 7, pp. 31711–31722, 2019. DOI: 10.1109/ACCESS.2019.2903723.

[22] M. Jaderberg, V. Dalibard, S. Osindero, W. M. Czarnecki, J. Don ahue, A. Razavi, O. Vinyals, T. Green, I. Dunning, K. Simonyan et al., "Population based training of neural networks," arXiv preprint arXiv:1711.09846, 2017.

[23] A. Li, O. Spyra, S. Perel, V. Dalibard, M. Jaderberg, C. Gu, D. Budden, T. Harley, and P. Gupta, "A generalized framework for population based training," in Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2019, pp. 1791 1799. DOI: 10.1145/3292500.3330649.

[24] M. Jaderberg, W. M. Czarnecki, I. Dunning, L. Marris, G. Lever, A. G. Castaneda, C. Beattie, N. C. Rabinowitz, A. S. Morcos, A. Ruder man et al., "Human-level performance in 3D multiplayer games with population-based reinforcement learning," Science, vol. 364, no. 6443, pp. 859–865, 2019. DOI: 10.1126/science.aau6249.

[25] D. Ho, E. Liang, X. Chen, I. Stoica, and P. Abbeel, "Population based augmentation: Efficient learning of augmentation policy schedules," in International Conference on Machine Learning. PMLR, 2019, pp. 2731–2741