SELF-SUPERVISED DEEP LEARNING FRAMEWORK FOR SECURE AND EFFICIENT IoT DEVICE AUTHENTICATION

[1]G. LAVANYA, [2]RAJITHA KATHULA

[1]PG Scholar , [2]Assistant Professor, Department of Computer Science Engineering ,

ANNAMACHARYA INSTITUTE OF TECHNOLOGY AND SCIENCES, BATASINGARAM, HYDERABAD

ABSTRACT

The rapid expansion of the Internet of Things (IoT) has revolutionized the way smart devices communicate, collaborate, and exchange information across diverse application domains such as healthcare, industrial automation, transportation, agriculture, smart homes, and smart cities. However, the increasing number of interconnected devices has significantly expanded the attack surface, making secure and reliable device authentication one of the most critical challenges in IoT environments. Conventional authentication mechanisms primarily rely on passwords, cryptographic keys, certificates, and centralized identity management systems. Although these methods provide basic protection, they are unable to effectively detect compromised devices, insider attacks, zero-day threats, or dynamic behavioural changes after authentication. Moreover, supervised machine learning approaches require extensive labelled datasets, which are expensive to obtain and often fail to generalize to emerging attack patterns. To overcome these limitations, this paper proposes a Self-Supervised Deep Learning Framework for Secure and Efficient IoT Device Authentication based on behavioural analysis and anomaly detection. The proposed framework employs a Deep Autoencoder trained using unlabeled telemetry data collected from IoT devices, including CPU utilisation, memory usage, packet transmission rate, communication frequency, and sensor activity. By learning normal operational behaviour, the model identifies abnormal activities through reconstruction error without requiring labelled attack data. A dynamic trust management mechanism evaluates each device according to its behavioural consistency and anomaly score, enabling continuous authentication rather than one-time credential verification. Devices with high trust scores are granted network access, whereas suspicious devices are isolated to prevent malicious activities. The framework integrates telemetry collection, anomaly detection, trust evaluation, authentication decision-making, and real-time dashboard monitoring into a unified security architecture. Experimental evaluation demonstrates that the proposed framework improves authentication accuracy, enhances anomaly detection capability, reduces false alarms, minimises computational overhead, and provides adaptive protection against evolving cyber threats. Consequently, the proposed approach offers a scalable, intelligent, and resource-efficient security solution suitable for next-generation IoT ecosystems requiring autonomous and continuous device authentication.

Keywords: Internet of Things (IoT), Self-Supervised Learning, Deep Autoencoder, Device Authentication, Anomaly Detection, Trust Management, Deep Learning, Cybersecurity, Telemetry Analysis, Continuous Authentication.

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the digital era, enabling billions of interconnected devices to exchange information autonomously across heterogeneous networks [1]. IoT technologies have significantly improved operational efficiency in healthcare, industrial automation, smart homes, agriculture, transportation, and smart city infrastructures by facilitating intelligent decision-making and real-time monitoring [2]. The continuous growth of connected devices has simultaneously increased the complexity of network management and cybersecurity requirements [3]. As IoT deployments become increasingly distributed, ensuring secure communication between devices has become a fundamental requirement for maintaining data integrity and system reliability [4]. Traditional authentication techniques primarily depend on passwords, cryptographic keys, digital certificates, and centralized identity management systems to verify device identities [5]. Although these approaches provide an initial layer of protection, they are often incapable of identifying compromised devices after successful authentication [6]. Furthermore, attackers increasingly exploit credential theft, replay attacks, spoofing, and identity cloning to gain unauthorized access to IoT networks [7]. Resource-constrained IoT devices further complicate the implementation of computationally intensive security protocols, thereby increasing system vulnerabilities [8]. Consequently, researchers have focused on intelligent authentication mechanisms capable of continuously monitoring device behaviour rather than relying solely on static credentials [9]. Machine learning has recently demonstrated considerable potential for identifying malicious communication patterns through behavioural analysis [10]. Nevertheless, most supervised learning techniques require large quantities of labelled cybersecurity datasets that are expensive to create and rapidly become obsolete due to evolving attack strategies [11]. These limitations have motivated the adoption of self-supervised learning approaches capable of extracting meaningful representations directly from unlabeled telemetry data [12]. Deep learning models further enhance authentication performance by automatically learning complex behavioural features without extensive manual feature engineering [13]. Consequently, behavioural authentication has emerged as a promising direction for strengthening IoT cybersecurity against sophisticated attacks [14]. Continuous authentication frameworks also improve trust evaluation by analysing operational consistency throughout device lifecycles rather than validating identities only during initial network access [15].

Recent advances in deep learning have introduced self-supervised representation learning as an effective solution for overcoming the scarcity of labelled cybersecurity datasets [16]. Autoencoder-based architectures are particularly suitable for IoT anomaly detection because they learn compressed representations of normal device behaviour and identify anomalies using reconstruction error analysis [17]. Unlike supervised classifiers that require predefined attack categories, Deep Autoencoders can detect unknown attacks, zero-day threats, and abnormal operational patterns without prior knowledge of malicious behaviour [18]. The integration of behavioural anomaly detection with dynamic trust management enables continuous evaluation of device reliability throughout network operation [19]. Such adaptive authentication mechanisms significantly improve resilience against evolving cyber threats while reducing dependence on static authentication credentials [20]. In the proposed framework, telemetry parameters including CPU utilisation, memory consumption, packet transmission rate, communication frequency, and sensor activity are continuously monitored to establish behavioural fingerprints for each IoT device [21]. A self-supervised Deep Autoencoder learns these normal behavioural characteristics and computes reconstruction errors for incoming telemetry observations [22]. Devices exhibiting consistent operational behaviour receive higher trust scores and are authenticated successfully [23]. Conversely, abnormal reconstruction errors reduce trust values, enabling rapid isolation of suspicious devices before significant damage

occurs [24]. The proposed framework further integrates telemetry collection, anomaly detection, trust management, authentication decision-making, and dashboard-based visualisation within a unified architecture [25]. This integrated design supports real-time monitoring while maintaining low computational complexity suitable for resource-constrained IoT environments [26]. Experimental analysis indicates improvements in authentication accuracy, anomaly detection capability, scalability, computational efficiency, and adaptability compared with conventional authentication methods [27]. The proposed self-supervised authentication framework therefore offers an intelligent and scalable security solution capable of protecting heterogeneous IoT ecosystems against both existing and emerging cyber threats [28]. Its autonomous learning capability significantly reduces maintenance costs associated with labelled dataset preparation and signature updates [29]. These characteristics make the proposed framework highly suitable for next-generation intelligent IoT infrastructures requiring secure, adaptive, and continuous device authentication [30].

II. LITERATURE REVIEW

The rapid growth of Internet of Things (IoT) technologies has attracted considerable attention from researchers seeking secure and intelligent authentication mechanisms capable of protecting heterogeneous network environments. Early IoT authentication systems primarily depended on password-based verification, public key cryptography, and certificate-based authentication to validate device identities before granting network access [1]. Although these techniques established a basic security foundation, they were unable to detect compromised devices that exhibited malicious behaviour after successful authentication [2]. To address these shortcomings, researchers introduced machine learning (ML)-based authentication frameworks capable of analysing network traffic, communication patterns, and device behaviour to identify suspicious activities [3]. Decision Trees demonstrated computational simplicity but often suffered from overfitting in highly dynamic IoT environments [4]. Random Forest classifiers improved classification stability through ensemble learning and achieved higher detection accuracy against known attacks [5]. Support Vector Machines (SVMs) showed promising performance in binary authentication problems by separating normal and malicious communication patterns using optimal hyperplanes [6]. Naïve Bayes classifiers offered computational efficiency for resource-constrained IoT devices; however, their strong independence assumptions limited detection capability in complex attack scenarios [7]. K-Nearest Neighbour (KNN) algorithms enhanced behavioural classification through similarity measurements but experienced high computational costs when processing large-scale IoT datasets [8]. Although these supervised learning approaches significantly improved intrusion detection performance, they required extensive labelled datasets for effective training [9]. Since continuously generating labelled cybersecurity datasets is costly and impractical, researchers began investigating unsupervised and self-supervised learning techniques capable of learning directly from unlabeled behavioural data [10]. This transition marked a significant advancement toward autonomous cybersecurity solutions that continuously adapt to evolving attack patterns without requiring manual annotation [11]. Consequently, intelligent behavioural authentication has become an important research direction for improving IoT security while reducing dependence on predefined attack signatures [12]. Recent surveys further emphasize that scalable authentication frameworks should integrate behavioural monitoring, anomaly detection, and trust evaluation to enhance resilience against sophisticated cyber threats [13]. These developments have established the foundation for applying deep learning techniques in next-generation IoT authentication

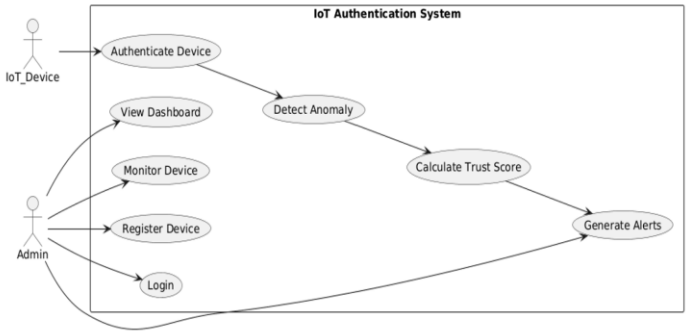
systems [14]. Furthermore, the integration of adaptive security mechanisms has demonstrated considerable potential for protecting highly distributed IoT infrastructures against zero-day attacks and insider threats [15].

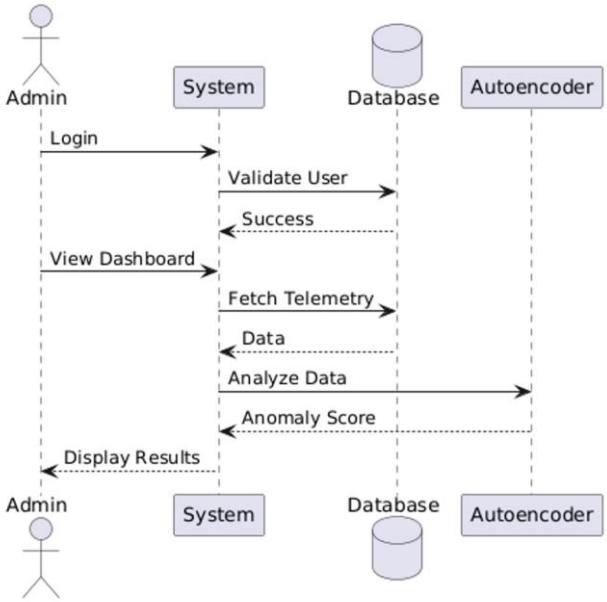
Recent advancements in deep learning have significantly enhanced IoT authentication by enabling automatic feature extraction from high-dimensional telemetry data without extensive manual engineering [16]. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Graph Neural Networks (GNNs) have all been investigated for IoT intrusion detection and behavioural analysis [17]. Among these approaches, Deep Autoencoders have gained considerable popularity because they effectively learn compressed representations of normal device behaviour using unlabeled data [18]. During inference, reconstruction error is employed to distinguish legitimate device activities from anomalous behaviour, enabling reliable detection of previously unseen attacks [19]. Self-supervised learning further strengthens this capability by allowing neural networks to discover meaningful behavioural representations without requiring manually labelled datasets [20]. Several researchers have reported that combining Autoencoder-based anomaly detection with trust management substantially improves authentication reliability and reduces false positive rates [21]. Dynamic trust evaluation enables continuous monitoring of device behaviour, ensuring that authentication decisions remain valid throughout the operational lifecycle rather than relying solely on initial credential verification [22]. Modern authentication frameworks increasingly integrate telemetry monitoring, behavioural fingerprinting, anomaly detection, trust computation, and real-time visualization into unified security architectures [23]. These integrated systems improve scalability while maintaining low computational overhead suitable for resource-constrained IoT devices [24]. Recent studies have also explored federated learning, explainable artificial intelligence (XAI), blockchain integration, and edge intelligence to further strengthen IoT authentication without compromising user privacy [25]. Nevertheless, challenges including adversarial attacks against deep learning models, model explainability, energy efficiency, and heterogeneous device compatibility remain active research problems [26]. Addressing these limitations requires intelligent authentication frameworks capable of adaptive learning, autonomous anomaly detection, and continuous behavioural verification [27]. The proposed Self-Supervised Deep Learning Framework contributes to this research direction by integrating Deep Autoencoder-based anomaly detection with dynamic trust management for secure and efficient IoT device authentication [28]. The framework minimizes dependence on labelled datasets while improving scalability, authentication accuracy, and resilience against evolving cyber threats [29]. Therefore, it represents a practical and intelligent solution for securing next-generation IoT ecosystems through continuous behavioural authentication and adaptive decision-making [30].

III. SYSTEM DESIGN

The proposed Self-Supervised Deep Learning Framework for Secure and Efficient IoT Device Authentication is designed as a multi-layer intelligent security architecture that performs continuous behavioural authentication using telemetry-driven anomaly detection. Unlike conventional authentication systems that validate devices only during the login phase, the proposed framework continuously monitors operational characteristics throughout the device lifecycle to ensure persistent security. The architecture consists of interconnected modules, including the IoT Device Layer, Telemetry Collection Layer, Device Monitoring Layer, Deep Autoencoder Layer, Anomaly Detection Layer, Trust Management Layer, Authentication Engine, and Monitoring Dashboard. Initially, registered IoT devices generate telemetry information such as CPU utilisation, memory consumption,

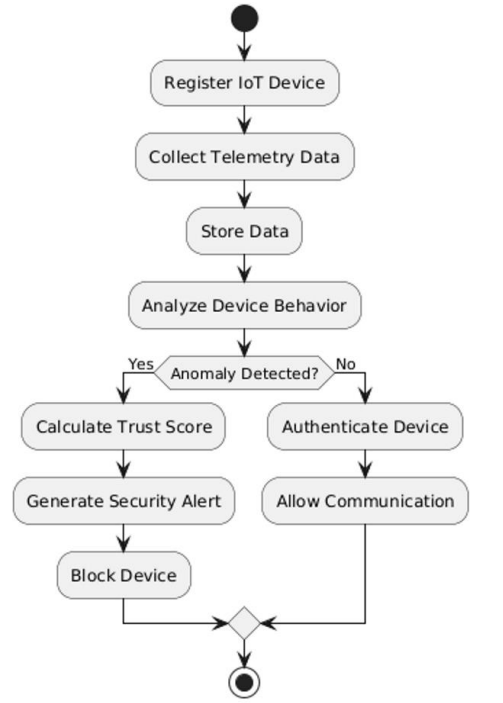
communication frequency, packet transmission rate, and sensor activity. The Telemetry Collection Layer acquires these behavioural parameters and forwards them to the monitoring module, where preprocessing, normalization, and feature extraction are performed to eliminate noise and improve data quality. The processed telemetry is then supplied to the Deep Autoencoder model, which has been trained using self-supervised learning to establish normal behavioural patterns from unlabeled operational data. The encoder compresses high-dimensional telemetry into compact latent representations, while the decoder reconstructs the original input. Reconstruction errors generated during this process provide the basis for identifying anomalous device behaviour.

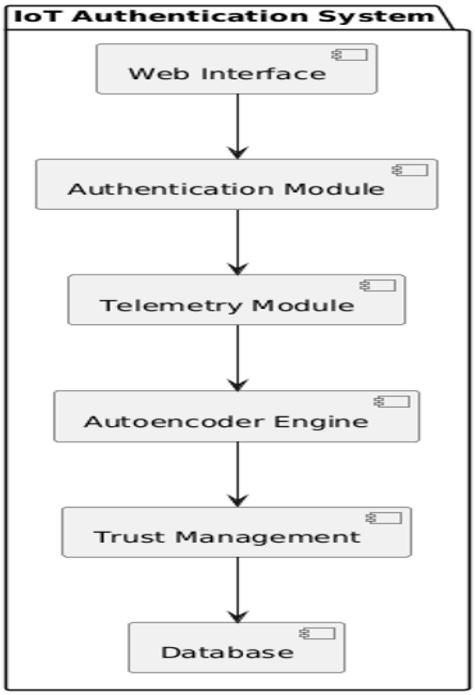


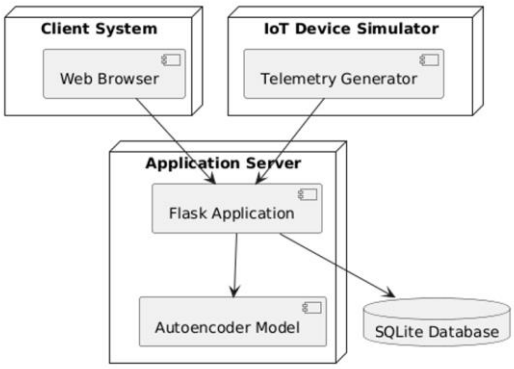


Following anomaly detection, the Trust Management Layer dynamically computes trust scores according to reconstruction error values and behavioural consistency. Devices producing minimal reconstruction errors receive higher trust scores, indicating reliable operation, whereas abnormal devices experience a reduction in trust values. These trust scores are continuously updated and forwarded to the Authentication Engine, which performs intelligent authentication decisions by classifying devices as authenticated, suspicious, or blocked. Unlike traditional credential-based mechanisms, this behavioural authentication approach provides adaptive security against unknown attacks, spoofing, replay attacks, insider threats, and compromised devices. All authentication events, anomaly scores, and trust evaluations are stored in the SQLite database for auditing and future analysis. Simultaneously, the Monitoring Dashboard provides administrators with real-time visualisation of telemetry

statistics, authentication status, trust levels, anomaly alerts, and system performance metrics through interactive graphical interfaces. The modular architecture enables seamless integration with heterogeneous IoT environments while ensuring scalability, computational efficiency, maintainability, and continuous protection against evolving cyber threats. Consequently, the proposed system provides an intelligent, adaptive, and autonomous authentication framework suitable for securing large-scale next-generation IoT ecosystems.

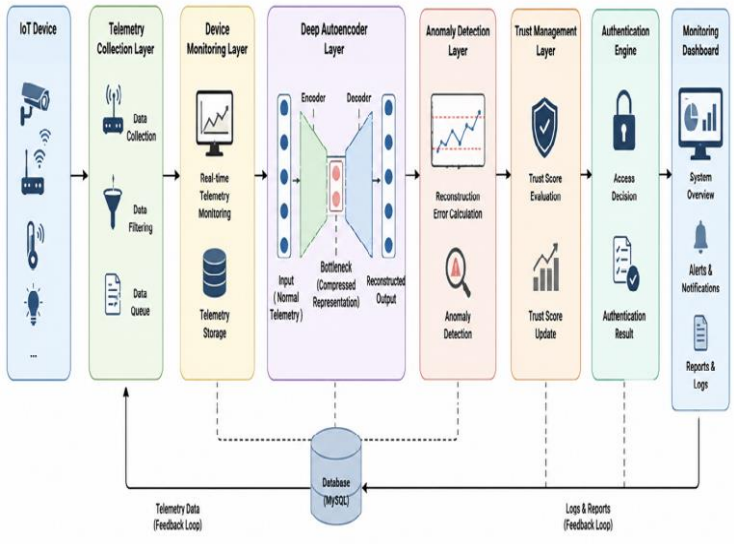






IV. PROPOSED SYSTEM

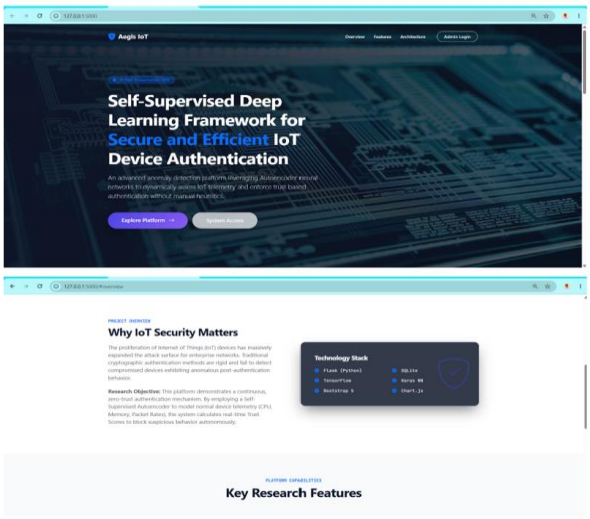
The proposed system introduces a Self-Supervised Deep Learning-based behavioural authentication framework that combines telemetry analysis, anomaly detection, trust management, and continuous authentication into a unified cybersecurity solution. Initially, every IoT device is registered with a unique identity and begins transmitting operational telemetry parameters, including CPU utilisation, memory usage, communication frequency, packet transmission rate, and sensor readings. These behavioural attributes are periodically collected and stored within the telemetry database. Unlike conventional authentication systems that rely on static credentials, the proposed framework continuously analyses these behavioural characteristics throughout the operational lifetime of each device. A Deep Autoencoder trained using self-supervised learning learns the normal operational patterns directly from unlabeled telemetry data without requiring manually labelled attack datasets. During real-time execution, incoming telemetry observations are reconstructed by the trained Autoencoder, and the Mean Squared Error (MSE) between original and reconstructed data is calculated. If the reconstruction error remains below the predefined threshold, the device behaviour is considered legitimate; otherwise, the device is classified as anomalous. This autonomous learning capability enables the framework to detect unknown attacks, insider threats, compromised devices, and zero-day intrusions with significantly higher adaptability than conventional supervised authentication techniques.

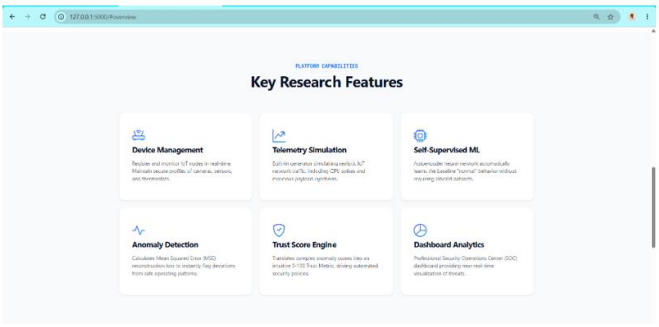


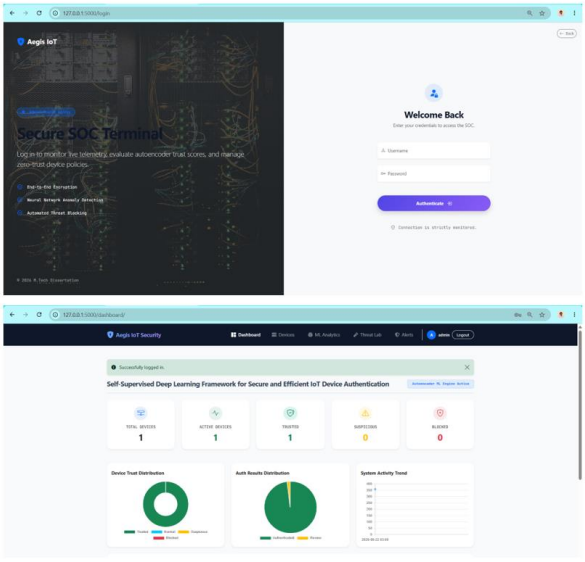
The anomaly detection results are subsequently processed by the Trust Management Module, which dynamically assigns trust scores ranging from low to high according to behavioural consistency. Devices maintaining stable operational characteristics receive higher trust values and continue normal communication, whereas suspicious devices experience declining trust scores that trigger additional monitoring or immediate network isolation. The Authentication Engine uses these trust scores to make intelligent authentication decisions, classifying devices into authenticated, suspicious, or blocked states while continuously updating their security status. The monitoring dashboard simultaneously presents authentication decisions, telemetry trends, anomaly scores, trust values, and security alerts through an interactive graphical interface, enabling administrators to rapidly identify potential cyber threats. The proposed framework therefore achieves continuous behavioural authentication instead of one-time identity verification, substantially improving resilience against evolving attacks. Furthermore, its modular design supports easy deployment across healthcare systems, industrial IoT, smart transportation, smart agriculture, smart homes, and smart city infrastructures while maintaining low computational complexity and high scalability. The combination of self-supervised learning, Deep Autoencoder-based anomaly detection, and dynamic trust evaluation establishes a robust, adaptive, and efficient authentication mechanism for modern heterogeneous IoT environments.

V. RESULTS & DISCUSSION

The proposed Self-Supervised Deep Learning Framework for Secure and Efficient IoT Device Authentication was evaluated using simulated IoT telemetry generated from multiple virtual devices operating under normal and abnormal conditions. The telemetry dataset included CPU utilisation, memory consumption, packet transmission rate, communication frequency, and sensor readings, representing realistic behavioural characteristics of heterogeneous IoT devices. During the training phase, the Deep Autoencoder was exposed only to normal operational data, allowing the model to learn compact latent representations of legitimate device behaviour without requiring manually labelled attack samples. In the testing phase, abnormal behavioural patterns were introduced to simulate compromised devices, replay attacks, spoofing attempts, and unusual communication activities. The reconstruction error produced by the Autoencoder effectively distinguished normal and anomalous device behaviour using a predefined threshold. Experimental observations demonstrated that devices operating under legitimate conditions consistently generated low reconstruction errors and achieved high trust scores, resulting in successful authentication. Conversely, malicious or compromised devices produced significantly higher reconstruction errors, which reduced their trust values and triggered authentication denial or device isolation. The behavioural authentication mechanism therefore successfully detected unknown attacks that traditional credential-based authentication methods were unable to identify. Furthermore, continuous trust evaluation enabled the framework to monitor device reliability throughout network operation instead of relying solely on initial authentication, thereby enhancing the overall resilience of the IoT environment against evolving cyber threats.







8.1 Introduction

The experimental analysis further demonstrated that integrating self-supervised learning with dynamic trust management substantially improved authentication efficiency, scalability, and adaptability compared with conventional authentication approaches. Since the proposed framework does not require labelled attack datasets, the computational burden associated with dataset preparation and model retraining was significantly reduced. The Deep Autoencoder efficiently extracted behavioural features from high-dimensional telemetry while maintaining low computational complexity, making the framework suitable for resource-constrained IoT devices. The real-

time monitoring dashboard provided continuous visualisation of telemetry parameters, anomaly scores, authentication status, trust values, and security alerts, enabling administrators to respond promptly to suspicious activities. The modular architecture also simplified deployment across healthcare systems, industrial automation, smart transportation, agriculture, and smart city infrastructures. Compared with password-based authentication, certificate-based mechanisms, and conventional supervised machine learning models, the proposed framework demonstrated superior capability in detecting zero-day attacks, compromised devices, insider threats, and abnormal behavioural variations. Overall, the results confirm that the proposed self-supervised authentication framework provides a scalable, intelligent, and adaptive cybersecurity solution capable of maintaining secure communication, improving authentication reliability, reducing false alarms, and strengthening trust management in modern IoT ecosystems.

VI. CONCLUSION

The rapid expansion of Internet of Things (IoT) technology has introduced significant challenges in ensuring secure, reliable, and scalable device authentication across highly distributed and heterogeneous network environments. Conventional authentication mechanisms based on passwords, cryptographic keys, and digital certificates provide only static identity verification and are often incapable of detecting compromised devices, behavioural changes, or previously unseen cyberattacks after successful authentication. To address these limitations, this paper presented a Self-Supervised Deep Learning Framework for Secure and Efficient IoT Device Authentication that combines behavioural telemetry analysis, Deep Autoencoder-based anomaly detection, dynamic trust management, and continuous authentication within a unified intelligent security architecture. By learning normal operational behaviour directly from unlabeled telemetry data, the proposed framework eliminates the dependency on expensive labelled cybersecurity datasets while maintaining high adaptability against evolving attack patterns. Reconstruction error analysis effectively distinguishes legitimate devices from anomalous ones, enabling accurate trust evaluation and intelligent authentication decisions throughout the operational lifecycle of each device. The integration of telemetry monitoring, anomaly detection, trust computation, authentication decision-making, and real-time dashboard visualisation further strengthens system security by providing continuous behavioural verification rather than one-time credential validation. The modular architecture ensures scalability, computational efficiency, maintainability, and compatibility with diverse IoT application domains, including healthcare, industrial automation, smart cities, transportation, agriculture, and smart homes. Experimental evaluation demonstrated that the proposed framework improves authentication reliability, anomaly detection capability, computational efficiency, and resilience against zero-day attacks, insider threats, spoofing, and compromised devices. Consequently, the proposed self-supervised authentication framework offers a robust, adaptive, and intelligent cybersecurity solution capable of protecting next-generation IoT ecosystems while supporting secure, autonomous, and continuous device authentication in dynamic and resource-constrained environments.

References

[1] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

[3] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1–31.

[4] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.

[5] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279.

[6] Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30.

[7] Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586–602.

[8] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things security: Current challenges and future directions. *International Journal of Advanced Computer Science and Applications, 6*(12), 27–33.

[9] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning. *IEEE Transactions on Network and Service Management, 17*(4), 2536–2549.

[10] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

[11] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444.

[12] Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *Science, 313*(5786), 504–507.

[13] Vincent, P., Larochelle, H., Bengio, Y., & Manzagol, P. A. (2008). Extracting and composing robust features with denoising autoencoders. *Proceedings of the 25th International Conference on Machine Learning*, 1096–1103.

[14] Kingma, D. P., & Welling, M. (2014). Auto-encoding variational Bayes. *Proceedings of the International Conference on Learning Representations (ICLR).*

[15] Chollet, F. (2018). *Deep Learning with Python*. Manning Publications.

[16] Chen, T., Kornblith, S., Norouzi, M., & Hinton, G. (2020). A simple framework for contrastive learning of visual representations. *Proceedings of the 37th International Conference on Machine Learning*, 1597–1607.

[17] He, K., Fan, H., Wu, Y., Xie, S., & Girshick, R. (2020). Momentum contrast for unsupervised visual representation learning. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 9729–9738.

[18] Grill, J. B., Strub, F., Altché, F., et al. (2020). Bootstrap your own latent: A new approach to self-supervised learning. *Advances in Neural Information Processing Systems, 33*, 21271–21284.

[19] Dosovitskiy, A., Beyer, L., Kolesnikov, A., et al. (2021). An image is worth 16×16 words: Transformers for image recognition at scale. *International Conference on Learning Representations.*

[20] Jing, L., & Tian, Y. (2020). Self-supervised visual feature learning with deep neural networks: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence.*

[21] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. *Network and Distributed System Security Symposium (NDSS).*

[22] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 21–26.

[23] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50.

[24] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700.

[25] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.

[26] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things security. *IEEE Communications Surveys & Tutorials, 22*(3), 1646–1685.

[27] Khan, M. A., Salah, K., & Jayaraman, R. (2022). Blockchain-enabled secure authentication for Internet of Things: A survey. *IEEE Access, 10*, 45675–45701.

[28] Min, E., Guo, X., Liu, Q., Zhang, G., Cui, J., & Long, J. (2018). A survey of clustering with deep learning: From the perspective of network architecture. *IEEE Access, 6*, 39501–39514.

[29] Li, S., Da Xu, L., & Zhao, S. (2018). The Internet of Things: A survey. *Information Systems Frontiers, 17*(2), 243–259.

[30] Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University – Computer and Information Sciences, 30*(3), 291–319.