International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Smart Web Attack Detection in IoT Using Multi-Model

Nallamothu Venkat Koushik,Jakku Sravana Venkata Karthik and Todupunuri Shivamani
Department of Information Technology
Sreenidhi Institute of Science and Technology
{venkatkoushiknallamothu,jakkukarthik24,shivatodupunuri}@gmail.com
Mr.KAMESHWAR REDDY R
Department of Information Technology
Sreenidhi Institute of Science and Technology
kameshwar.r@sreenidhi.edu.in

***Abstract*— The objective of this research paper is the soaring increase of the. Internet of Things (IoT) has posed serious security threats. on our critical infrastructure systems. Devices with limited resources have a tendency of transmitting information without any sending. properly checking the payload. The present paper presents a. new Zero-Trust IoT Broker Architecture that uses Ensemble The Deep Learning methods, such as CNN, LSTM, and. MRN, along with AES-128 encryption, which is secure adequate to use with blockchain. The Zero-Trust Architecture uses an early-fusion hybrid "Max-Confidence" Ensemble. Network on ingestion layer to detect and remove. harmful payloads, such as XSS, SQL, and Path Traversal attacks, until they arrive at the central repository of clouds. The ensemble network has superior accuracy to. When tested on, the results of F1-score were compared to other models. various attack datasets. The encrypted storage layer guarantees that information stored is consistent post- ingestion.**

***Index Terms*— Internet of Things (IoT), Blockchain, Ensemble Deep Learning, CNN-LSTM, Web Attack Detection, AES Encryption, Zero-Trust, Data Immutability**

INTRODUCTION

The swift development of IoT has transformed the character of. it infrastructures by offering a highly-connected en. the environment, where devices are going to be in billions. IoT Equipments present a colossal amount of information at an unbelievable rate. rate–s Smart cities to automation in industry and indi. monitoring devices of individual health-making up the basis. to support real-time decision-making as well as big data analytics.

Although the growth of IoT devices has tremendously surpassed. the amount, the development of special security measures. of diversity in communication patterns and the quantity. it is made possible by the amount of computing power that can be accessed by the IoT devices. unrealistic to implement conventional firewalls and antivirus pro. grams aimed at supporting classical networks to protect IoT. networks. Traditionally system security has been centred on. implementing extensive application level protection, but, the continuous rise of new threats is now making. a security void far into which our advanced is today. cyber criminals are already on the move.

The most recent issue in the threat landscape that is concerning. has popped up–stuffing bad web payloads within. otherwise-ordinary communication flows with trusted IoT devices. Attackers leverage well-known vulnerabilities (i.e., Cross-site Scripting (XSS) and SQL In) SQLi (SQLi) to directly embed malicious SQL snippets. into streams of IoT devices which can then interact with other devices in the IoT or develop sensor. charts as a by-product of their work. These malicious communications, which are sent via trusted communica. tions channels, are not perceived by the traditional network. filtering methods at levels until they are ultimately stored. SAFE in a central cloud based repository of an enterprise. tory and/or database. This may be done by corrupted data. tion, rogue user accounts and/or system. crashes. Even if detection mechanisms have been put there are still risks which are in place in these systems. For example, when an attacker can access a database with a configured detection mechanism, the attacker can then retroactively action against records that were previously obeyed. the database, and making the chain of trust null. required in such critical applications like those needed in to give correct reports or those of the medical field. be in a position to conduct adequate financial audits.

Given all these various security issues surrounding IoT devices, this study has created a new security architecture that can be used to counter them all the security issues: the dual shield security architecture. This is a dual shield solution that can be used as part of the Zero Trust paradigm of IoT and suggests a significant shift in the existing security architecture by offering an Intelligent Web Security Architecture With Advanced Ensemble Deep Learning Based Web Attack Detection System (EDL-WADS) and an Immutable Cryptographic Pipeline. These components serve as one intelligence gateway to all data entering it and use the principle of verify first, trust second in processing all such incoming data. Hybridized and advanced A.I. machine learning techniques, namely Convolutional Neural Networks (CNN) to understand the space aspect, Long Short-Term Memory (LSTM) to understand the time

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

aspect and Multi-Resolution Networks (MRN) to identify the structural anomaly attacks, will ensure that the rate at which all forms of attack vectors are detected gets as high as possible within this architecture. Also, once the data are confirmed as valid, it will directly be encrypted using Block Chain (BLOCKCHAIN GRADE) AES-128 encryption and OTP (One-Time Password) based access tokens, hence leaving the entire dataset uncryptographically unalterable and, consequently, resistant to unauthorized interference in the corresponding Cloud Storage Layer. Thus, the dual shield security architecture is an end-to-end solution to the entire set of security challenges that exist on the IoT networks in every country worldwide and, as a consequence, offers a remedy to the current IoT Security Crisis.

LITERATURE SURVEY

The blistering development of Internet of Things (IoT) systems has made the contemporary network environment extremely complicated, posing acute cybersecurity issues. With the billions of devices going online the issue of secure communication and securing data is of paramount importance. To control such problems, scholars have undertaken to combine complex technologies like Artificial Intelligence (AI) and Decentralized Ledger Technologies (DLT), especially blockchain, to enhance intrusion identification and data integrity. At the beginning phases, IoT security was predominantly based on the use of traditional Intrusion Detection Systems (IDS) that employed signature-based methods to recognize known assaults. However, these systems were not effective in handling the diverse nature of IoT devices and protocols. The articles by Al-Fuqaha et al. (2020) noted the complexity of dealing with heterogeneous IoT environments, and Kumar et al. (2020) proposed early monitoring mechanisms, such as EDIMA, to enhance detection. As noted by Khan et al. (2021), these and similar efforts however not only limited traditional firewalls and rule-based systems, but demonstrated that these systems also do not detect advanced attacks embedded in a network payload.

The way out of these constraints was to introduce machine learning into the IoT security systems. Machine learning also offered automation as well as enhanced detection in comparison to the traditional approach. But it was quickly seen that a single model would not do. Zhou et al. (2021) proved that, in particular, support vector machines (SVM) tend to deliver high false positive scores, when it comes to zero-day attacks, including cross-site scripting (XSS). This demonstrated that the systems should be more intelligent and adaptive. Sikos et al. (2021) highlighted the need to have semantic-aware intrusion detection systems capable of learning the context of network traffic, as opposed to pattern matching. Additionally, Sharma et al. (2022) pointed out that the lack of standardized and high-quality datasets negatively impacts the performance and generalization ability of machine learning models in IoT environments.

As cyber attack patterns grew more complexified, the researchers shifted their focus to deep learning methods which can capture complex and non-linear trends in big datasets. Convolutional neural networks (CNN) were commonly used to extract spatial image features of network traffic making it possible to identify concealed attack patterns. Meanwhile, Long Short-Term Memory (LSTM) networks were found to be very useful in examining temporal trends, and so, can be applied to slow and continuous attacks like botnets. These models were shown to be effective in enhancing detection accuracy by researchers, such as Roopak et al. (2021) and Diro et al. (2021). Hybrid models were incorporated to improve further performance even more, using several methods of deep learning. As an example, Ullah et al. (2022) used CNN models together with GRU in network classification to detect more quickly and accurately. Other methods featured were autoencoders and dimensional data reduction, which were used to minimize data dimensions and dynamic and adaptive threat response via deep reinforcement learning. Recent research has also addressed the implementation of these models on the edge as opposed to a cloud-based system. Edge-based detection systems also minimize latency and respond more quickly, which are why they are more appropriate to real-time applications in IoT systems. Even though deep learning enhanced the level of detection, the use of a single model proved to be risky, particularly in complicated scenarios of attacks. To counter this problem, scientists proposed ensemble learning algorithms where several models are used to enhance the overall performance. Ensemble procedures have been shown to be more dependable since failures of single models are minimized. Research by Gao et al. (2022) revealed that multi-model ensembles can offer efficient protection to smart grid systems, whereas the study by Khraisat et al. (2023) has exhibited that the combination of CNN and LSTM models offers a superior coverage with respect to various kinds of attacks. The methods of AdaBoost and stacking were also employed to achieve a better detection rate and prioritize high-confidence alerts. Ferrag et al. (2024) emphasized the tendency of ensemble models to be resistant to adversarial attacks, in which attackers seek to control the model. Moreover, the recent studies have paid attention to the creation of lightweight outfit models which are able to be efficiently executed on the resource-limited IoT devices. Latif et al. (2024) and Hosen et al. (2024) demonstrated that these models could be effective in achieving high detection accuracy and low computational overhead which is a good reason to consider them in practice when they need to be used in the real world.

Conversely, to guarantee the security and integrity of stored data, in conjunction with attack detection, has also become a top priority in the IoT. The attack still can be detected and even after it is detected, unless it can be proven that the data stored cannot be manipulated or altered, the system is still at risk. To counter this, blockchain

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

technology has been much tapped as a decentralized and secure counter. Immutability, transparency and trust are some of the characteristics that blockchain offers and this makes it an appropriate line of defence against sensitive IoT data. Christidis et al. (2020) showed the ability of blockchain to create a trustworthy chain of custody of existing IoT data to ensure that any transactions are safely documented. Dorri et al. (2021) suggested solutions to be implemented in smart home environments that require using lightweight blockchain solutions, whereas Reyna et al. (2022) suggested ways to combine blockchain and IoT to share data more safely. Privacy-preserving models and systems based on smart contracts were presented by other researchers to automate security procedures. As an illustration, Ali et al. (2023) suggested the use of smart contracts that block malicious nodes automatically, whereas Pavithran et al. (2023) introduced an addition of AES-128 encryption to blockchain networks to provide confidentiality to data. Research works by Singh et al. (2024) affirmed that it was possible to implement such encryption methods in real time IoT applications. There has also been an application of blockchain in avenues including healthcare, where tight control of sensitive data is of the essence. Dwivedi et al. (2024) illustrated the application of blockchain in securing medical IoT, where the recent study by Tuli et al. (2025) examined sophisticated implementations of AI, blockchain, and up-to-date communication systems.

Even though the given field has made a great move forward, a number of crucial problems are still left. A big weakness is that most of the systems available mostly concentrate on the detection accuracy but not the security of data saved. Ensemble and deep learning models prove very useful in detecting attacks, yet they tend to make the assumption that storage systems under the system are secure. Conversely, blockchain-related solutions are aimed at the data storage reinforcement but presuppose that the data coming in is trusted. This is a critical loophole since even the ill data can be enshrined forever in the blockchain unless it has been authenticated first. So, it is obvious that more complex and holistic approach to detecting and secure storage is needed.

Further system development that will help reduce this gap is one that uses a zero-trust architecture in which all data must be validated prior to storage. It can be done through integrating ensemble deep learning models to detect attacks accurately and against insecure encoding with cryptographic and blockchain-based models to keep the data safe. Such a system would prevent storage and propagation of malicious data in addition to identifying attacks. By making sure that only confirmed data has been logged, this method can greatly increase the level of security and reliability of the IoT systems in general. This underscores the need to come up with holistic solutions which can travel beyond detection to offer end to end security in the contemporary distributed environments.

PROPOSED SYSTEM

This system is named as Blockchain-Augmented Ensemble Deep Learning Framework of Secure IoT Data Ingestion, and is aimed at enhancing the security of IoT environments through enhanced detection mechanisms coupled with safe data storage. In most of the existing system there is no separation of data verification and data storage, this provides security holes. This project will address this problem by introducing a single, zero-trust pipeline in which data is verified and then stored securely. The general architecture is built in such a way that verifiable or malicious data does not penetrate the system, thus enhancing reliability as well as security.

This has the pre-ingestion layer which is the first component of the system that serves as a gatekeeper to incoming data. IoT devices tend to transmit data in formats such as JSON or CSV, and attackers can conceal malicious code in data formats. The system employs ensemble deep learning model to identify such hazards, which involves multiple components that are collaborative. A Convolutional Neural Network (CNN) is employed to learn patterns of the data, character by character, it is capable of recognizing attacks such as cross-site scripting. Concurrently, Long Short-Term Memory (LSTM) model is able to examine the sequence and context of the information which assist in detecting intricate attacks like SQL injection. Moreover, a multi-resolution network will be employed to identify structural anomalies, which other models might not very easily recognize. All these models operate simultaneously to scan all incoming data packets.

The decision-making process is considered to be one of the most important aspects of this layer. The system does not involve averaging results of all models, instead it employs a maximum confidence method. In case any of the models identify a threat with high confidence, the data is rejected instantly. This will assist in preventing attacks that even come in the system to be detected. The suspicious data is kept on a different storage to be analyzed further without compromising the system and losing any other valuable data to be investigated in future.

After the check-up of the data is done in the first phase, it is transferred to the second stage, which is concerned with secure storage. In this stage, the system uses encryption techniques along with blockchain-inspired concepts to ensure data integrity. Prior to storing data, it is encrypted with AES 128 converting it into a format that cannot be read. This will make sure that upon a hacker (who might access the storage system) does not easily comprehend or misuse the data. The system also ensures an unalterable record of the data stored, in that once the data is saved, it could not be changed. This will assist in avoiding meddling and guarantee that the information is reliable with time.

The last level of the system is concerned with the guaranteed access to the stored information. Conventional systems mostly make use of uncomplicated authentication

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

techniques such as usernames and passwords that are easily hacked. To enhance security, this system brings up the two-step system of verification. Once a user demands

getting access to the data, an OTP is created and is delivered to the user via an email. This takes into consideration the fact that only authorized users can access the data. Also, the system will verify the alteration of the data prior to access. In case of any changes detected, they are denied access, making sure that only unchanged and valid data is availed to the user.

On the whole, the system proposed is proactive in securing IoT as the combination of detection, encryption, and access control is presented in one structure. This is unlike the conventional systems which solely consider detecting attacks, as in this case, malicious data is not kept anywhere. The system incorporates the idea of deep learning, encryption, and blockchain to offer a more comprehensive and efficient solution to ensuring the security of IoT data. This renders it flexible and applicable in contemporary applications in which huge amounts of data must undergo processing in a secure and efficient manner.

Algorithm 1

Function *EnsemblePredictor.predict(S)* **is**

Input: Raw payload string S
Output: Boolean is_attack, confidence score
Step 1: Initialization
Load CNN M_{cnn}
Load LSTM M_{lstm}
Load MRN M_{mrn}
Step 2: Parallel Processing
$Score_{cnn} = M_{cnn}.predict(S)$
$Score_{lstm} = M_{lstm}.predict(S)$
$Score_{mrn} = M_{mrn}.predict(S)$
Step 3: Fusion
$Score_{ens} = \max(...)$
Step 4: Decision
if $Score_{ens} \geq 0.80$ **then**
    $is\_attack = TRUE$
else
    $is\_attack = FALSE$

Algorithm 2

Function *secure_storage_and_access(D)* **is**
    Input: Validated data D
    Output: Secure storage and controlled access
    Stage A: Secure Ingestion (Vaulting)
    Step 1: Encryption
    Initialize AES-128-CBC with key K
    $Cipher\_Data = AES\_Encrypt(D, K)$
    Step 2: Persistence
    Append ".enc" to filename
    Store $Cipher\_Data$ on disk
    Step 3: Status
    Data enters immutable state
    Stage B: Zero-Trust Access
    Step 4: Request
    User requests file F
    Step 5: Authentication Challenge
    Generate 4-digit OTP
    Store OTP in session
    Send OTP via SMTP email
    Step 6: Verification
    Capture $User\_OTP$
    if $User\_OTP == OTP$ **then**
        Proceed to decryption
    else
        Deny access
    Step 7: Final Decryption
    Load $Cipher\_Data$ and key K
    $Decrypted\_D = AES\_Decrypt(Cipher\_Data, K)$
    Serve $Decrypted\_D$ to user

EXPERIMENTATION ANALYSIS AND RESULTS

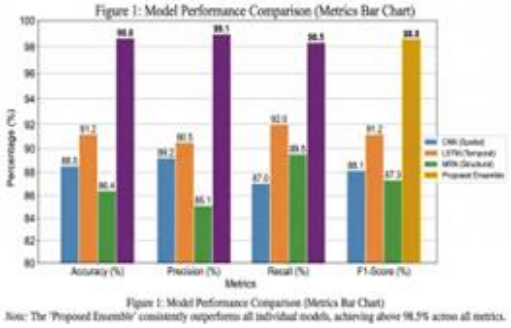

Fig. 1. Model Performance Comparison (Bar Graph)

CONCLUSIONS

As emphasized in this paper, to create a safe IoT system that safeguards data against cyber-attacks, there must be a concerted effort in terms of developing intelligent

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

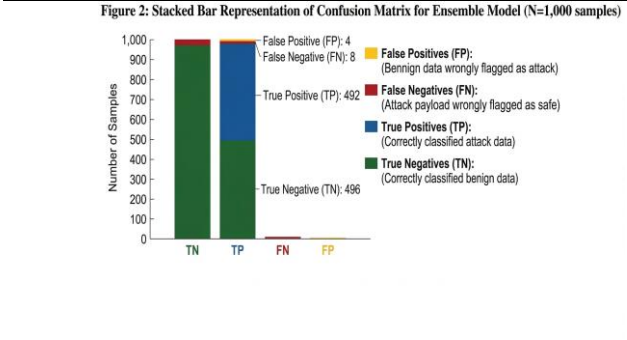

Fig. 2. Confusion Matrix Representation

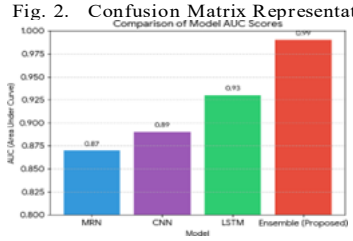

Fig. 3. AUC Score Comparison Graph

threat detection and trusted persistence of data. Current literature is considering intrusion detection and data storage as two distinct issues, which creates gaps in end-to-end security. The suggested architecture incorporates CNN-LSTM-MRN ensemble model of pre-ingestion checks with cryptographic immutability provisioned by the AES algorithm and access control supported by OTPs. This will create a synchronous zero-trust pipeline which blocks entry of malicious data but ensures confidentiality plus integrity. In this way, the system takes the IoT security beyond an industrial defensive response to engineered protection that can be verified and can be deployed at scale.

Moreover, ensemble deep learning can be used to detect attacked patterns with greater robustness by detecting both spatial and temporal, as well as structural patterns, simultaneously. Max-Confidence voting mechanism acts as a way of guaranteeing that threats detected to some extent do not access the system beforehand: a large number of false negatives are minimized. As opposed to the traditional methods of IDS, this technique will not only enhance the accuracy but also enhance the resilience to advanced and masked payload attacks that are an inherent feature of contemporary IoT setting.

Moreover, by combining cryptographic storage with controlled access, the validated data can be tamper-proof and accessible safely. There is strict access policy that is supported by use of pre-storage encryption and OTP-authentication to meet the principles of zero-trust. On the whole, the proposed system offers a scaled, secure, and intelligent framework, bridging the gap between detection and persistence, and it is very appropriate in the next-generation smart city and industrial IoT applications.

Future Work

Future development can be dedicated towards improving the framework suggested, adding light and fashionable deep learning models that can be deployed on edge and fog computing platforms. As IoT devices might have very limited computational and energy resources, edge deployment of the CNN-LSTM-MRN ensemble will benefit scalability and latency minimization. Besides, it can also consider some of the techniques like model pruning, quantization, and federated learning, which would allow distributed and privacy-preserving training on a set of IoT nodes.

The other direction that is significant is the incorporation of the advanced blockchain mechanisms and smart contracts in order to further automatize security policies. Future systems may adopt the fully decentralized architectures based on smart contracts that dynamically execute access control, threat responses, and isolation of nodes instead of providing a pseudo-blockchain approach. In addition, the explainable AI (XAI) methods will be included to assist in the interpretation of model decisions, making the system more transparent and reliable to the administrators and regulatory compliance.

Lastly, it is possible to consider the incorporation of future technology like quantum-resistant cryptography and AI-based adaptive security models in future studies. The system can be expanded as cyber threats spread, and can be used to aid self-learning capabilities in order to adapt to emerging patterns of attack in real-time. Assessment of the framework on high-scale real-life data and application in smart cities or industrial IoT scenarios will further confirm its performance, strength, and feasibility.

References

[1] M. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies," IEEE Commun. Surveys, 2020.
[2] A. Kumar, S. Jain, and P. Sharma, "EDIMA: Early Detection IoT Monitoring Architecture," IEEE Access, 2020.
[3] M. A. Khan, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, 2021.
[4] Y. Liang and J. Chen, "Machine Learning-Based Vulnerability Detection in IoT Systems," IEEE IoT Journal, 2020.
[5] Y. Zhou et al., "Support Vector Machine-Based Intrusion Detection Systems for IoT," IEEE Access, 2021.
[6] L. F. Sikos, "Cybersecurity in IoT: Semantic-Based Intrusion Detection," IEEE Trans. Industrial Informatics, 2021.
[7] P. Sharma et al., "Edge-IIoTset: A New Dataset for IoT Intrusion Detection," IEEE DataPort, 2022.
[8] M. Roopak, G. Yun Tian, and J. Chambers, "Deep Learning Models for IoT Intrusion Detection," IEEE Access, 2021.
[9] G. Diro and N. Chilamkurti, "Distributed Attack Detection Using LSTM," IEEE Trans. Dependable Secure Comput., 2021.
[10] I. Ullah and Q. Mahmoud, "Hybrid CNN-GRU Model for Intrusion Detection," Future Internet, 2022.
[11] A. Popoola et al., "Autoencoder-Based Intrusion Detection Systems," IEEE Access, 2022.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

TABLE I
COMPARISON BETWEEN EXISTING WORK AND PROPOSED SYSTEM

Criteria	Existing Work (Literature Survey)	Proposed Work
Architecture Approach	Mostly isolated systems focusing either on IDS or blockchain separately	Integrated end-to-end pipeline combining detection, storage, and access control
Detection Technique	Signature-based IDS, ML models (SVM), or single DL models (CNN/LSTM)	Ensemble Deep Learning (CNN + LSTM + MRN) with parallel scanning
Accuracy & False Positives	High false positives in single models and poor zero-day detection	Max-Confidence Voting reduces alert dilution and improves detection accuracy
Attack Coverage	Limited to specific attacks like SQLi or botnets	Covers multi-vector attacks such as XSS, SQLi, Command Injection, and Directory Traversal
Feature Extraction	Uses either spatial (CNN) or temporal (LSTM) features	Combines spatial, temporal, and structural feature extraction
Ensemble Strategy	Uses averaging or stacking methods	Uses Max-Confidence Strategy (early fusion) for faster rejection
Handling Malicious Data	Only detects and generates alerts	Immediate rejection and storage in secure AttackLog
Data Storage Method	Traditional databases or blockchain without validation	AES-128 encrypted pseudo-blockchain storage
Data Integrity	Blockchain ensures immutability but assumes input data is safe	Ensures validated, encrypted, and immutable storage
Security Model	Reactive (detects attacks after occurrence)	Proactive Zero-Trust security model
Encryption Usage	Limited or applied after storage	Pre-storage encryption using AES-128-CBC
Access Control	Username/password-based authentication	OTP-based dual-factor cryptographic access
Trust Model	Implicit trust in incoming IoT data	Zero-Trust model (no data trusted before validation)
Pipeline Integration	Detection and storage are separate processes	Synchronous pipeline (Detection → Encryption → Access)
Research Gap Handling	Does not address connection between detection and persistence	Bridges gap with detection-before-blockchain approach
Scalability for IoT	Limited due to inefficiency or latency issues	Designed for high-volume heterogeneous IoT environments
Defense Against Advanced Attacks	Weak against adversarial or masked payloads	Strong due to multi-layer deep learning and cryptographic sealing

[12] M. Abdel-Basset et al., "Deep Reinforcement Learning for Cybersecurity," IEEE Network, 2022.
[13] W. Susilo et al., "Character-Level CNN for SQL Injection Detection," IEEE Access, 2023.
[14] A. Alrashdi et al., "FB-IDS: Edge-Based Intrusion Detection System," IEEE Access, 2023.
[15] Y. Gao et al., "Ensemble Learning for Smart Grid Security," IEEE Trans. Smart Grid, 2022.
[16] A. Khraisat et al., "Survey on Intrusion Detection Systems: Ensemble Methods," IEEE Access, 2023.
[17] M. Al-Zewairi et al., "AdaBoost-Based Deep Learning for Cybersecurity," IEEE Access, 2023.
[18] M. A. Ferrag et al., "Adversarial Machine Learning in IoT Security," IEEE Communications Surveys, 2024.
[19] S. Latif et al., "Lightweight Ensemble Learning for IoT Devices," IEEE Access, 2024.
[20] M. Hosen et al., "Stacked Ensemble Models for Intrusion Detection," IEEE Access, 2024.
[21] N. Mendis et al., "Multi-Resolution Networks for Cyber Threat Detection," IEEE Access, 2025.
[22] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for IoT," IEEE Access, 2020.
[23] A. Dorri et al., "Blockchain for IoT Security and Privacy," IEEE IoT Journal, 2021.
[24] A. Reyna et al., "Blockchain and IoT Integration: Survey," Future Generation Computer Systems, 2022.
[25] I. Makhdoom et al., "PrivySharing: Privacy in Blockchain-Based IoT," IEEE Access, 2022.
[26] M. Ali et al., "Smart Contract-Based IoT Security Framework," IEEE Access, 2023.
[27] S. Pavithran et al., "AES-Based Secure Blockchain Framework," IEEE Access, 2023.
[28] R. Singh et al., "Performance Evaluation of AES in IoT," IEEE Access, 2024.
[29] A. Dwivedi et al., "Blockchain for Secure Medical IoT Systems," IEEE Access, 2024.
[30] S. Tuli et al., "AI-Quantum Blockchain for 6G IoT," IEEE Network, 2025.
[31] X. Zhang et al., "CNN-LSTM Hybrid Model for Network Intrusion Detection," IEEE Access, 2021.
[32] J. Kim et al., "Web Attack Detection Using Deep Learning," IEEE Access, 2022.
[33] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[34] NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.
[35] J. Kindervag, "Build Security into Your Network's DNA: The Zero Trust Model," Forrester Research, 2010.