International Journal of Multidisciplinary Research and Growth Evaluation.

Ferdowsi University Mashhad/ The second International Conference
Artificial Intelligence: Between Scientific Innovation and Human Responsibility

A Multi-Network Blockchain-Enhanced Deep Belief Network Approach for Intrusion Detection

Ahmed Aljabri [1*], **Farah Jemili** [2], **Ouajdi Korbaa** [3]
[1-3] Université de Sousse, ISITCom, MARS Research Laboratory, LR17ES05, 4011 Hammam Sousse, Tunisia
[1] University of Mustansiriyah, Baghdad, Iraq

* Corresponding Author: **Ahmed Aljabri**

Article Info

ISSN (Online): 2582-7138
Impact Factor (RSIF): 7.98
Volume: 06
Issue: 06
November - December 2025
Received: 29-09-2025
Accepted: 31-10-2025
Published: 27-11-2025
Page No: 56-65

Abstract

This paper presents a novel approach to cybersecurity by integrating blockchain technology, RSA hashing, and deep learning techniques to enhance data security and intrusion detection. We employ Differential Evolution (DE) for intelligent data selection from blockchain, ensuring that sensitive information is securely managed. The data is then partitioned into training and testing sets through a Money-grubbing Simulated Annealing algorithm, optimizing the dataset for model performance. A Deep Belief Network (DBN) is utilized to predict and classify potential intrusions with high accuracy, leveraging its ability to detect complex patterns in large datasets. Our method ensures robust data integrity and security through blockchain, while simultaneously achieving superior classification precision in intrusion detection tasks. Experimental evaluations and simulations validate the effectiveness of the proposed system, demonstrating significant improvements in both security and performance. This work highlights the potential of combining blockchain- based data security with advanced machine learning models, offering a scalable and efficient solution to the growing challenges in cybersecurity.

Keywords: Intrusion Detection System (IDS), Blockchain Technology, Deep Belief Networks (DBN), RSA Hashing, Multi-Network Security.

1. Introduction

The design of embedded real-time systems is evolving rapidly with the increasing integration of critical functionalities for surveillance applications, particularly in the biomedical, environmental, aeronautics, and mobile communication systems. These systems face significant challenges, especially in minimizing energy con- Sumption while ensuring robust security. The extensive use of blockchain technology has added complexity to intrusions against cloud-based systems, making traditional security measures less effective (Khan, 2023) [18]. For instance, hackers have briefly controlled more than half of the worldwide mining hash rate for each coin due to weaknesses in cryptocurrency networks (Kariri, 2022) [15]. Blockchain technology, also known as distributed ledger technology, serves as the foundation for numerous applications that provide data privacy and trust ser- vices across various sectors. It enables trustworthy, transparent, and irreversible transactions and information sharing among users. Beyond the financial sector,

blockchain's potential applications include the energy sector (Khalil, 2022) [17], Internet of Things (IoT) (Almajed *et al.*, 2022) [5], supply chain and manufacturing (Evsutin *et al.*, 2022) [9], personal data protection (Yuvaraj, 2021) [24], large dataset analysis (Trivedi & Patel, 2022) [22], and data anomaly detection (Hannah, 2022) [12].

Blockchain is poised to bring about significant societal changes and is widely acknowledged as one of the most transformative technological advances (Almajed *et al.*, 2022) [5]. Im- mutable records provided by distributed transactions involving IoT devices and Cyber-Physical Systems (CPSs) can be generated automatically by devices (Evsutin *et al.*, 2022) [9]. However, cloud computing introduces concerns related to data security and trust management among cloud service providers (Bouachir *et al.*, 2020) [6]. The public, distributed, and au- tonomous nature of cloud computing can create trust issues when working with components from multiple companies. Privacy and security concerns often make cloud service providers hesitant to share data or disclose breaches (Wang *et al.*, 2021) [23].

Developing a collaborative intrusion detection system (CIDS) to detect both in- ternal and external threats is crucial. Novel cyberattacks on a large number of cloud nodes should be inexpensive and scalable. Betrayal attacks (Zhao *et al.*, 2018) [25] by hos- tile nodes collaborating to send false information can impede alarm aggregation, diminishing its effectiveness. Blockchain-based security and operational studies in the CPS sector have been made public, focusing on specific aspects of CPS functioning or security enhanced by blockchain technology (Chang, 2021) [7].

This study proposes a novel approach that combines blockchain-based data security with Deep Belief Networks (DBNs) and RSA hashing. By utilizing the RSA hashing technique to generate blocks, we ensure immutable transaction records. The data secured by blockchain is divided into testing and training datasets, allowing the model to be trained and tested with input from both sources. The primary contribution of our approach lies in the integration of blockchain technology with Deep Belief Networks (DBNs) and RSA hashing to develop a secure, scalable, and intelligent intrusion detection framework tailored for cloud-based Cyber-Physical Systems (CPSs). Unlike traditional systems that treat security and anomaly detection separately, our method ensures end-to-end data integrity through immutable blockchain records while enabling intelligent threat detection via deep learning. The RSA hashing mechanism reinforces trust by securing data blocks, and the DBN model effectively identifies complex attack patterns using training and testing datasets derived from blockchain-secured inputs. This holistic design not only mitigates internal and external threats—including betrayal attacks but also offers a lightweight, distributed, and collaborative solution addressing the unique privacy and trust challenges inherent in cloud-based CPS environments. Overall, our approach represents a significant advancement in unifying secure data management with adaptive cyber threat detection mechanisms for real-time embedded systems. This paper is organized into five main sections. Section 2 provides a detailed background and reviews the state of the art. Section 3 examines the proposed approach, highlighting the benefits and guiding principles of the employed techniques. Section 4 presents the experimental results, evaluates opportunities and challenges, and discusses the findings. Finally, Section 5 concludes with a comprehensive analysis and outlines potential future directions.

2. Related Works

A blockchain A blockchain network may serve as the backbone of a decentralized system, according to (Afanasev *et al.*, 2018) [1]. To achieve this objective, intelligent contracts must be designed to provide dependable bidirectional communication between network nodes. The authors argue that Ethereum's blockchain is prefer- able for CPPS networks due to its development potential and robust features. [20] introduced a publication model that uses blockchain technology to protect the confidentiality of critical material while enabling devices to ex- change data with network nodes. This publish/subscribe paradigm, based on blockchain technology, employs public-key encryption and an equality test to circumvent trust issues and eliminate the chance of a single point of failure.

Explained the concept of intrusion detection systems (IDSs) and demonstrated their applicability in cloud environments (Hajimirzaei & Navimipour, 2019) [11]. They high- lighted how the deep design of bitcoin enables privacy measures for smart con- tracts and distributed intrusion detection. Researchers also utilized Extended Short-Term Memory (ESTM), a deep learning method, to detect attacks, show- casing the potential of advanced machine learning techniques in enhancing IDS capabilities (Krishnaveni, 2021) [19].

Researchers led by (Gao, 2018) [10] examined the evolution of blockchain technology and its applications in smart cities. They reviewed various blockchain techniques currently used in IoT applications, identifying potential challenges and proposing solutions for further research (Karuppusamy, 2022) [16].

Also discussed the potential use of blockchain technology in cloud trading (Mishra *et al.*, 2018) [20]. They provided a brief history of blockchain, its current applications, and the possible privacy and security risks associated with blockchain-based cloud trading. Despite the virtualization and diverse components of CIDSs, cloud providers can share information about potentially dangerous application behaviors and event logs. However, the effectiveness of shared data depends on the reliability and interoperability of SIEM systems.

Designing a CID system that works well in the cloud involves addressing unique features such as detecting threats both inside and outside the company while minimizing false positives and negatives. Scale-out features that work with var- ious data middle designs and are based on the cloud are essential. Ensuring maximum security resilience against zero-day vulnerabilities (Aljabri *et al.*, 2024; Jemili, 2022) [3, 14] is crucial for protecting users' privacy, authentication, and data integrity across all ICDS- participating systems. IDSs in the same cloud domain that trust each other can share information and report intrusions collaboratively. However, malicious or hacked nodes that add bias to the data can hinder the gathering of alerts (Alkadi *et al.*, 2020) [4]. Intrusion detection systems face challenges in dealing with real-time data trans- fer across multiple cloud providers due to the need to protect user privacy and prevent data destruction.

Advocates of using blockchain technology to enhance the security of intrusion detection systems (IDS) in wireless sensor networks (WSNs) presented a method to increase the reliability and transparency of intrusion detection procedures (Hasan, 2018) [13]. Utilizing a blockchain-based method guarantees the permanence and honesty of intrusion detection data, enhancing the precision and reliability of threat detection and response. However, this method's higher computing workload and resource use might affect the efficiency and expandability of the IDS in limited- resource WSN settings. Additionally, blockchain technology adds complexity and potential weaknesses that advanced attackers might target, necessitating strong security measures to protect the integrity and confidentiality of blockchain-based IDS systems.

Table 1: Related Work Comparison.

Study	Focus	Approach	Advantages	Limitations
(Afanasev *et al.*, 2018) [1]	Decentralized Systems	Intelligent Contracts on Ethereum Blockchain	Reliable bidirectional communication	Development fully realized potential not
	Data Confidentiality	Blockchain-based Pub-lish/Subscribe Model	Protects eliminates failure critical single material, point of	Implementation complexity
(Hajimirzaei &Navimipour, 2019) [11]	Cloud IDS	ESTM Method Deep Learning	Privacy measures for smart contracts, distributed IDS	High computational requirements
(Gao, 2018) [10]	Smart Cities	Blockchain Evolution and Applications	Identifies challenges and solutions for IoT applications	Limited focus on real-time performance
(Mishra *et al.*, 2018) [20]	Cloud Trading	Blockchain for Privacy and Security	Addresses privacy and security risks	Scalability issues
(Hasan, 2018) [13]	WSN Security	Blockchain-based IDS	Increases reliability and transparency	High computing workload, re- source use
(Samad *et al.*, 2020) [21]	Healthcare Security	Blockchain with IDS	Protects patient data privacy, system integrity	Integration complexity, processing overhead
(da Silva *et al.*, 2017)	Smart Grid Security	Blockchain with IDS	Detects unauthorized access, data tampering	High investment, Computational overhead

In the healthcare sector, a new method was introduced to improve security by Combining blockchain technology with IDS (Samad *et al.*, 2020) [21]. This solution addresses the distinct security concerns of healthcare 4.0, which involves integrating digital technologies such as IoT devices, electronic health records (EHRs), and telemedicine. The IDS can efficiently identify and mitigate risks to patient data privacy and system integrity by leveraging blockchain's decentralized and unchangeable characteristics. However, incorporating blockchain technology into existing health- care systems require substantial investment in financial resources and technological expertise. The processing overhead from blockchain processes might impact real-time threat detection and response in critical healthcare settings.

Similarly, a revolutionary method was introduced to enhance security in smart grid systems by integrating blockchain technology with IDS (Samad *et al.*, 2020) [21]. This approach addresses the growing cybersecurity risks targeting smart grid infrastructures, crucial components of contemporary energy distribution networks. The IDS can efficiently detect and prevent harmful actions, including unauthorized access, data tampering, and denial-of-service attacks, by leveraging blockchain's decentralized and unchangeable characteristics. However, incorporating blockchain technology into existing smart grid systems requires significant investment in financial resources and technical expertise. The computational overhead of blockchain processes might impede real-time threat detection and response in dynamic smart grid scenarios.

In summary, while blockchain technology offers significant advantages in enhancing the security and resilience of various systems, it also presents challenges that need to be addressed. Future research should focus on optimizing the integration of blockchain with IDS to improve scalability, efficiency, and real-time performance across different applications (Table 1). Our contribution introduces a hybrid approach that combines blockchain technology with Deep Belief Net- works (DBNs) and RSA hashing to enhance security and predictive intrusion detection. By utilizing Differential Evolution (DE) for efficient data handling and model training, our method addresses the challenges of real-time threat detection and response across various applications, including healthcare and smart grids. This approach not only improves scalability and performance by optimizing resource use but also integrates advanced cryptographic techniques to ensure robust data security. Our solution stands out by effectively balancing the need for high security, efficiency, and real-time performance, making it a significant advancement over existing methods.

3. Proposed Contribution

Although there has been a lot of development in the subject of blockchain technology-based approaches for multi-network intrusion detection security and privacy, several critical gaps remain that need to be addressed (Aljabri *et al.*, 2023, 2024) [1, 2]. Potential re- search gaps in this field include the need for more efficient and scalable solutions that can handle the high computational overhead associated with blockchain processes. Additionally, there is a lack of comprehensive studies on the integration of blockchain with advanced machine learning techniques, such as Deep Belief Networks (DBNs), to enhance predictive capabilities and real-time threat detection. Another significant gap is the challenge of ensuring data privacy and security while maintaining high performance and low latency in diverse and dynamic network environments.

Furthermore, the complexity of incorporating blockchain technology into existing systems, such as healthcare and smart grids, requires substantial investment in financial resources and technical expertise, which has not been thoroughly explored. Addressing these gaps will be crucial for developing robust, efficient, and scalable blockchain-based intrusion detection systems that can effectively protect against evolving cyber threats.

The proposed architecture presents an innovative, three-pronged approach that combines blockchain technology, deep learning, and evolutionary algorithms to ensure both data security and effective intrusion detection. The first prong of the approach focuses on securing the information using blockchain, with a particular emphasis on the RSA hashing algorithm. This ensures that all data stored in the blockchain is tamper-proof and immutable. The RSA hashing technique is Crucial in protecting data integrity as it involves encrypting the block headers and appending new blocks to the chain in a secure and distributed manner. The encryption is done by calculating the hash value of the block header, and the algorithm continues iteratively until the hash meets the predetermined tar- get value. This process guarantees that every transaction is cryptographically secure and resistant to tampering, thus preventing unauthorized access or malicious interference in the system.

The second prong involves the use of a classifier model designed to predict potential cyberattacks within the intrusion detection data (IDD). This model is powered by a Deep Neural Network (DNN), which is adept at processing complex patterns in large datasets. To enhance the model's performance, the data selection process is guided by a greedy evolutionary algorithm. This multi-objective approach allows for optimal feature selection, ensuring that only the most relevant data is used for training the model. By selecting the most informative features, the system reduces the computational load and improves the accuracy of the DNN model in predicting potential threats.

Finally, the third prong focuses on improving the efficiency of the system by using the RSA hashing mechanism to secure the blockchain and enable a collaborative and scalable approach to intrusion detection. The RSA algorithm ensures that each new block added to the blockchain is verified for integrity and consistency with the rest of the network. This mechanism not only ensures the security of the data but also fosters a decentralized, trustless environment for managing intrusion detection across multiple nodes. Each block is independently verified, ensuring that all participants in the system can confidently trust the transaction history without relying on a centralized authority.

Together, these three components—blockchain encryption, DNN-based intrusion detection, and evolutionary data selection—create a robust and resilient architecture that addresses key challenges in real-time intrusion detection for cloud-based Cyber-Physical Systems (CPSs). The system is not only scalable and lightweight, but it also enhances security and trust, providing a novel solution to the growing complexities of securing distributed systems in various critical domains such as healthcare, environmental monitoring, and mobile communication.

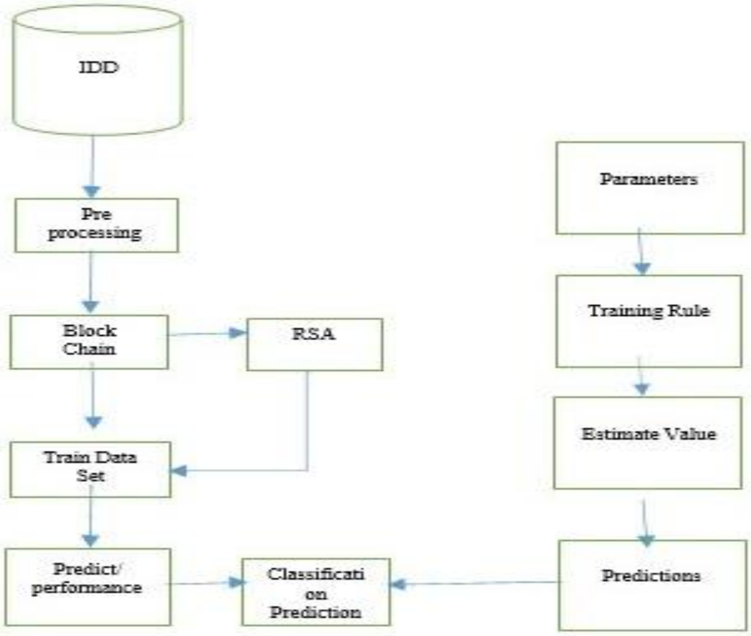

Fig 1: Proposed Contribution

4. Implementations

4.1. RSA Hashing Algorithm

This paves the way for the next evolution of encryption. In addition, public-key cryptography offers a new theoretical and technical basis for the development of future cryptography algorithms. It has developed into a vital component of the network that supports the information security industry. The RSA algorithm is widely considered to be the most secure implementation of public-key cryptography currently available. With discrete hashing, a public key is changed to a new integer. RSA private and public key generation consists of the following steps:

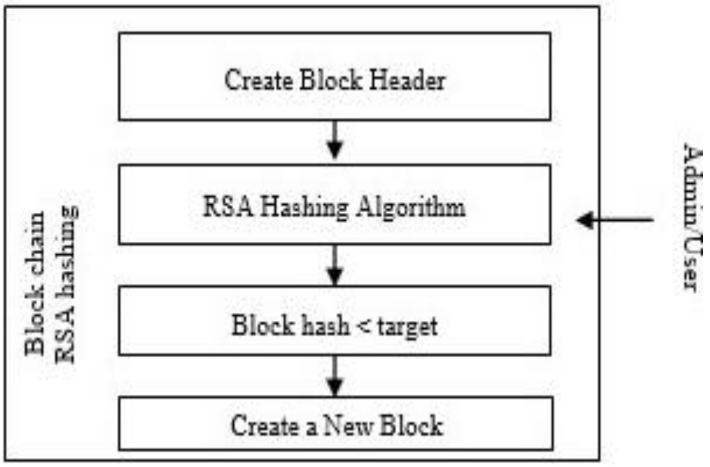

Fig 2: BC Using Block Creation.

$$e \times d \equiv 1\ (mod\Phi(n))$$

Step 1: Pick p and q, both of which are prime numbers that are extremely prime, at random.
Step 2: Compute n = p × q, Φ(n) = (p − 1) (q − 1); where Φ(n) is Euler's totient function.
Step 3: Select a public key e at random such that 1 < e < Φ(n) and gcd (e, Φ(n)) = 1; this indicates that both e and Φ(n) are coprime.
Step 4: Find the private key d such that:

4.2. SHA-256 Hashing Algorithm

This work is an important addition to the body of research that led to the creation of the SHA-256 hashing algorithm. Both the SHA-256 algorithm and its block diagram are carefully examined. Each SHA-256 technique can be evaluated based on its pre-hash and post-hash steps. Padding and m-block parsing are two essential parts of preparing a message. At the first stage of hashing, certain configuration settings must be established. With the hash and the padded message, a message schedule can be created. The message digest is the result of this calculation when the message is used as the input. By repeatedly making a message schedule, functions, constants, and word operations, a hash value can be obtained. The security features of the SHA-256 hash algorithm increase linearly with the size of the hash.

The Verilog programming language was used to implement SHA-256. The counter, message schedule, constant, multiplexer, compression function, and the SHA-256 module that outputs compressed data are all high-level components of the SHA- 256 architecture.

Figure 3 shows this same layout of a SHA-256 hash algorithm. The incoming data is split into 15 frames of 32 bits each, and an additional bit is appended at the end to create a 32-bit output. The remaining 64 bits are used to indicate the length of the message by utilizing the unselected bits. The SHA-256 hashing algorithm processes a message of 512 bits. A counter module is responsible for creating the message sequence. In SHA-256, the compression step is repeated 64 times to produce a single hash result.

Before processing the message, the SHA-256 hash technique requires a multiplexer module to generate eight distinct buffer initializations. Accessing the ROM blocks is necessary to determine the value of the constant Kt. These ROM blocks include both 32-bit and 64-bit ROMs in this persistent array. At the final stage, the output module generates a SHA-256 hash of the message. The output of the SHA-256 compression technique is used to set up the buffers, ensuring that the data is compressed as efficiently as possible. Message schedulers, like the one shown in Figure 3, are used to determine the SHA-256 Wt value of a message. For timestamps between 0 and 15, the entire input message is used. When t is between 16 and 63, the following equation is used to calculate Wt.

$$W_t = \sigma_1(W_{t_{-2}}) + W_{t_{-7}} + \sigma_0(W_{t_{-15}}) + W_{t_{-16}} \qquad (1)$$

Where σ0 and σ1 are defined as:

$$\sigma_0(x) = (x >> 7) \oplus (x >> 18) \oplus (x >> 3) \qquad (2)$$

$$\sigma_1(x) = (x >> 17) \oplus (x >> 19) \oplus (x >> 10) \qquad (3)$$

The message schedule for SHA-256, Wt, is defined as follows:

- For 0 ≤ t < 16, Wt is the input message.
- For 16 ≤ t < 64, Wt is calculated using the above equation.

This detailed process ensures the integrity and security of the hashed message.

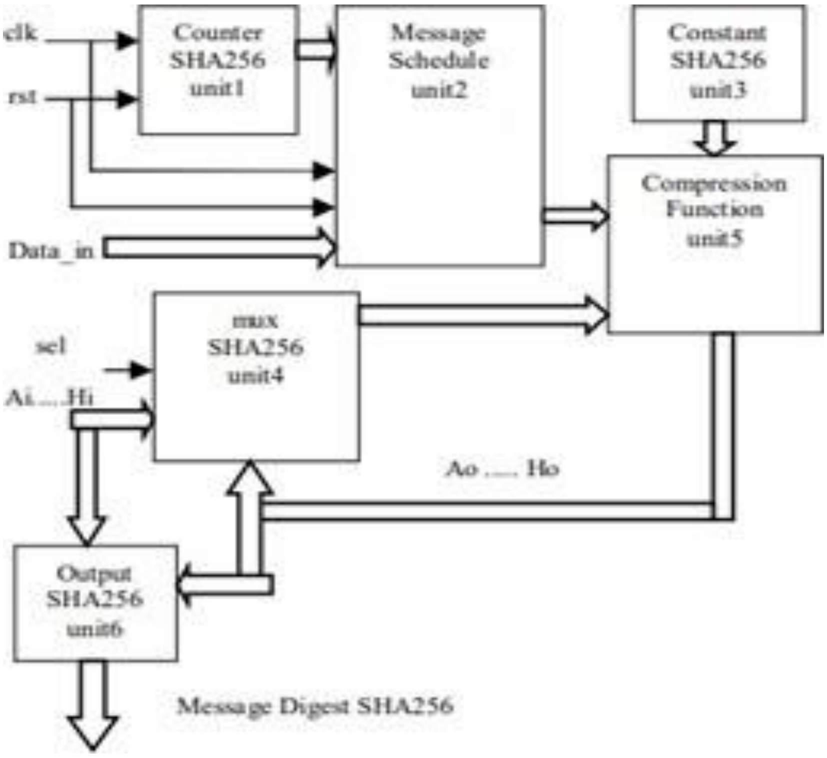

Fig 3: SHA-256 Hash Function Architecture.

4.3. DBN for Intrusion Prediction

Deep Belief Networks (DBNs) are a type of deep learning model composed of multiple layers of Restricted Boltzmann Machines (RBMs) and an additional classifier at the top. RBMs are stochastic neural networks that can learn a probability distribution over their set of inputs. They consist of a visible layer (rep- resenting the input data) and a hidden layer (representing latent features), with symmetric connections between these layers. RBMs are energy-based models that define a joint distribution between the visible and hidden units using an energy function.

The training of DBNs involves a greedy layer-wise unsupervised training method, which allows for the efficient training of multiple RBMs. This method trains one layer at a time, starting with the first RBM. Once the first RBM is trained, its hidden layer activations are used as the input for training the next RBM. This process is repeated for each subsequent layer, effectively stacking the RBMs to form a deep network. This layer-wise training approach enables the DBN to learn hierarchical feature representations from the data.

After the unsupervised pre-training of the RBMs, the DBN undergoes a super- vised fine-tuning phase. During this phase, the parameters of the entire network are fine-tuned using labeled data to improve the accuracy of the network’s classifications. This is typically done using backpropagation, where the gradient of the loss function with respect to the network’s parameters is computed and used to update the weights.

The fine-tuning process adjusts the weights of the network to minimize the classification error, leveraging the features learned during the unsupervised pre- training. This combination of unsupervised pre-training and supervised fine- tuning allows DBNs to achieve high classification performance, especially in scenarios with limited labeled data.

RBMs, being energy-based models, only consider the interactions between the visible and hidden layers, ignoring the interactions within the visible layer and within the hidden layer. The energy function of an RBM is defined as:

$$E(v,h) = -\sum_i a_i v_i - \sum_j b_j h_j - \sum_{i,j} v_i W_{ij} h_j \qquad (4)$$

Where v represents the visible units, h represents the hidden units, a and b are the biases for the visible and hidden units, respectively, and W is the weight matrix connecting the visible and hidden units.

The probability of a visible vector v and a hidden vector h is given by the Boltzmann distribution:

$$P(v,h) = e - E(v,h)\ Z\ (5)$$

Where Z is the partition function, ensuring that the probabilities sum to one. By stacking multiple RBMs and fine-tuning the network, DBNs can effectively learn complex data distributions and perform accurate classifications.

5. Experimentations

In this section, to evaluate the hypotheses and methods mentioned above, the experiments were conducted on a state-of-the-art computing platform consisting of a head node and commodity compute nodes equipped with high-performance hardware and software components. This platform was supplied with a high- speed multi-core CPU and a dedicated graphics processing unit (GPU), ensuring effective and rapid calculation of the established blockchain-based model and the assessment of its performance.

The DE-RSA-DBN simulations were conducted using a robust cloud infrastructure equipped with 15,557,842 KB of RAM, an Intel Xeon 2.3 GHz CPU, and a Tesla K80 GPU.

These high-performance settings were essential for running the simulations efficiently and effectively. The cloud infrastructure provided the necessary computational power to handle the complex calculations and data processing required for the simulations.

To evaluate the performance and advantages of the DE-RSA-DBN model com- pared to standard Intrusion Detection Systems (IDS), we utilized a Platform as a Service (PaaS) environment. This environment mimicked the operational conditions of both DE-RSA-DBN and standard IDS, allowing for an objective comparison of their performance. We set the difficulty levels for the public blockchains to 5, 6, and 10 for blockchains 1, 2, and 3, respectively. These difficulty levels were chosen to effectively simulate the conditions of both a blockchain and a traditional system. The varying difficulty levels allowed us to assess the performance of the DE-RSA-DBN model under different levels of computational complexity and security requirements.

For the training of the Deep Belief Network (DBN) model, we used data from intrusion samples obtained from the Kaggle repository. These samples provided a diverse and comprehensive dataset for training the DBN model, ensuring that it could learn to detect a wide range of intrusion types. The use of real-world data from Kaggle helped to validate the effectiveness of the DE-RSA-DBN model in practical scenarios (Table 2) (Fig. 4).

Table 2 presents a comparative analysis of the detection rate for various intrusion detection approaches across different numbers of attackers. The proposed DE-RSA-DBN method consistently outperforms existing techniques, including SPS, CPSMCS, and SD-CPS. Notably, the detection rate of the proposed model increases steadily from 0.915 to 0.960 as the number of attackers rises from 20 to 100. This improvement highlights the robustness and adaptability of the pro- posed method in accurately identifying intrusions, even under increasing attack intensity.

Table 2: Detection Rate Vs Number of Attackers for Different Methods

Number of Attackers	SPS	CPSMCS	SD-CPS	Proposed DE-RSA-DBN
20	0.885	0.895	0.905	0.915
30	0.890	0.900	0.915	0.925
40	0.895	0.905	0.920	0.930
50	0.900	0.910	0.925	0.935
60	0.905	0.915	0.930	0.940
70	0.910	0.920	0.935	0.945
80	0.915	0.925	0.940	0.950
90	0.920	0.930	0.945	0.955
100	0.925	0.935	0.950	0.960

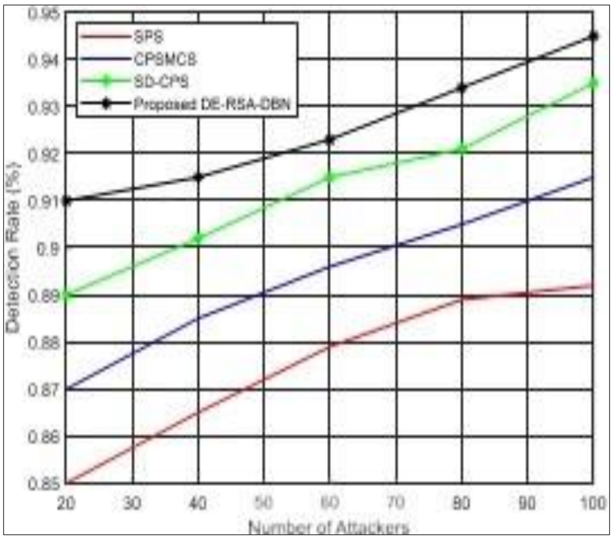

Fig 4: Detection Rate.

The simulations involved running the DE-RSA-DBN model on the cloud infrastructure, processing the intrusion samples, and evaluating the model's performance in terms of accuracy, efficiency, and security. By comparing the results with those of standard IDS, we were able to highlight the advantages of the DE- RSA-DBN approach, including its ability to handle complex data, its robustness against various types of intrusions, and its overall performance improvements.

6. Discussion

Through The DE-RSA-DBN approach introduces significant enhancements to traditional intrusion detection systems (IDS) by leveraging blockchain technology. One of the primary advantages of this approach is the immutability and completeness of the intrusion samples used by the IDS. Traditional methods of- ten struggles with ensuring the integrity and reliability of the data, which can lead to inaccuracies in intrusion detection. In contrast, the DE-RSA-DBN method ensures that the data remains unaltered and comprehensive, thereby improving the overall effectiveness of the IDS.

Table 3 compares the time consumption of five intrusion detection methods as the number of attackers increases. The proposed GGA-MD5H model consistently requires significantly less computation time than traditional approaches.

Table 3: Time Consumption (MS) Comparison Across Different Ids Approaches.

Number of Attackers	EMERALD	DOMINO	PIER	CIDS	Proposed GGA-MD5H
10	325	325	320	330	255
20	320	320	315	325	260
30	325	315	320	340	270
40	320	320	330	335	265
50	370	330	310	310	250
60	325	315	320	320	260
70	325	325	330	325	250
80	330	335	320	320	265
90	340	335	320	330	270
100	310	315	310	310	250

Such as EMERALD, DOMINO, PIER, and CIDS. While other methods show fluctuations and even increased time with more attackers, the proposed solution maintains a relatively stable and low execution time, ranging between 250 ms and 270 ms. These results demonstrate the efficiency and scalability of the pro- posed method, making it suitable for real-time intrusion detection in resource- constrained environments.

The blockchain architecture employed in DE-RSA-DBN surpasses public blockchains in verifying newly acquired data blocks. A public blockchain node releases an auditing statement after confirming a block's signatures, calculating the block's Proof of Work (PoW), and signing the validated contents.

This process involves checking the signature, creating a hash using the current block and the preceding block, and finally signing the hash. This rigorous verification process ensures the integrity and authenticity of the data, which is crucial for accurate intrusion detection.

Our experiments demonstrated that the DE-RSA-DBN model outperforms standard IDS in several key areas. By simulating attacks that resemble regular data, we were able to trick a normal IDS into misclassifying these attacks. However, the DE-RSA-DBN model, trained using the same methods and setups, was able to accurately detect these intrusions. This highlights the superior accuracy and robustness of the DE-RSA-DBN approach.

Table 4 illustrates the precision rate achieved by various intrusion detection systems under increasing numbers of attackers. The proposed GGA-MD5H approach consistently surpasses traditional methods such as EMERALD, DOMINO, PIER, and CIDS in terms of precision. While existing techniques gradually im- prove with more attackers, the GGA-MD5H model demonstrates a steeper and more stable rise in precision, reaching up to 97 Figures 5-6 illustrate the effectiveness of DE-RSA-DBN in detecting intrusions. The experimental results and simulations clearly show that DE-RSA-DBN offers significant advantages in terms of performance, efficiency, and security. The time consumption and precision rate metrics further emphasize the importance of our contribution. The DE-RSA-DBN model not only improves the accuracy of intrusion detection but also enhances the overall security and reliability of the system.

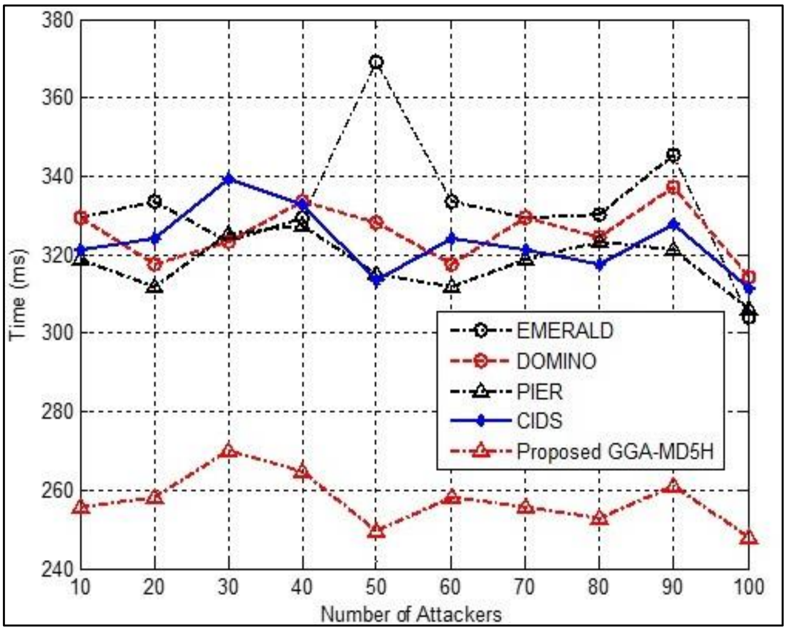

Fig 5: Time Consumption.

The DE-RSA-DBN approach marks a significant advancement in intrusion detection, combining the strengths of blockchain technology, Deep Belief Networks (DBNs), and RSA hashing to address the critical limitations of traditional intrusion detection systems (IDS). One of the main advantages of this approach lies in its integration of blockchain, which ensures the immutability and security of the data stored for intrusion detection. Blockchain's distributed and decentralized nature helps prevent tampering and unauthorized access to data, establishing a transparent and trustworthy foundation for intrusion detection. Coupled with RSA hashing, which strengthens the cryptographic security of the blockchain, this approach provides a solid framework for managing the integrity of the in- trusion detection dataset, making it more resistant to manipulation compared to traditional systems.

The use of Deep Belief Networks adds another layer of sophistication to the detection process. DBNs, with their ability to learn hierarchical patterns and representations from complex datasets, are particularly effective in detecting novel or sophisticated cyberattacks. Their capacity to process large volumes of data while accurately identifying attack patterns enhances the reliability of the intrusion detection system. When combined with blockchain-secured data, DBNs become even more powerful, as the model operates on a dataset that is guaran- teed to be authentic and secure, free from tampering.

Moreover, the introduction of a greedy evolutionary algorithm for data selection optimizes the intrusion detection process by intelligently selecting the most relevant features for training the DBN. This not only reduces computational complexity but also ensures that the model is trained on the most pertinent information, improving both its efficiency and accuracy. The multi-objective nature of the algorithm further enhances the system's capability to adapt to various threat scenarios, allowing it to effectively detect a wide range of attacks with minimal false positives.

The experimental results validate the strength of this approach in real-world settings. By demonstrating its ability to outperform traditional IDS models in both detection accuracy and efficiency, the DE-RSA-DBN framework proves to be a robust solution capable of handling the dynamic and complex nature of modern cyber threats. The integration of blockchain, deep learning, and evolutionary algorithms sets a new standard for intrusion detection in cloud-based Cyber-Physical Systems (CPSs), offering a scalable, secure, and effective method for addressing evolving security challenges.

In summary, the DE-RSA-DBN approach represents a promising direction for enhancing cybersecurity in real-time, embedded systems, where secure and timely detection of intrusions is crucial. Its ability to combine cutting-edge technologies in a cohesive framework provides a valuable contribution to the ongoing efforts in improving the resilience and trustworthiness of critical systems across various sectors.

Table 4: Precision Rate Comparison Across Different IDS Approaches.

Number of Attackers	EMERALD	DOMINO	PIER	CIDS	Proposed GGA-MD5H
10	0.83	0.84	0.85	0.86	0.92
20	0.84	0.85	0.86	0.87	0.93
30	0.85	0.86	0.87	0.88	0.935
40	0.86	0.87	0.88	0.89	0.94
50	0.85	0.86	0.87	0.88	0.945
60	0.86	0.87	0.88	0.89	0.95
70	0.87	0.88	0.89	0.90	0.955
80	0.88	0.89	0.90	0.91	0.96
90	0.88	0.89	0.90	0.91	0.965
100	0.89	0.90	0.91	0.92	0.97

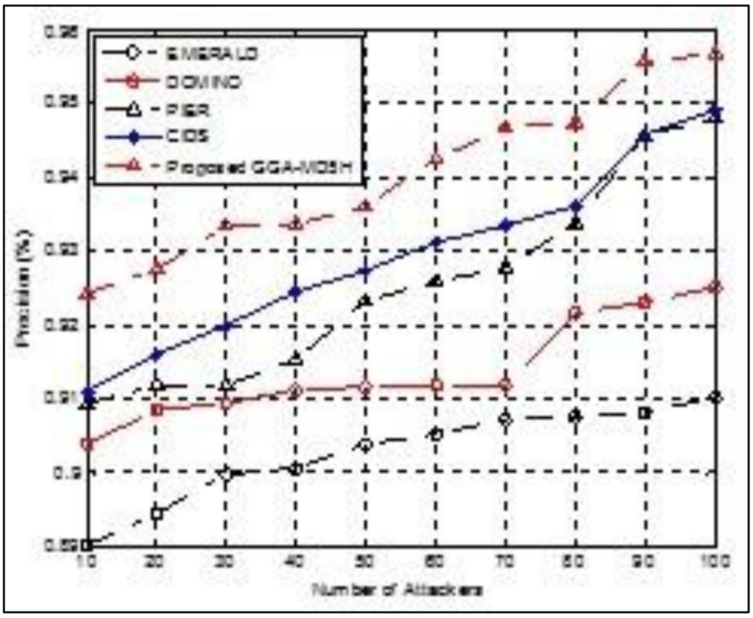

Fig 6: Precision Rate

7. Conclusion

To In this study, we proposed a novel approach that leverages blockchain technology, RSA hashing, and Deep Belief Networks (DBNs) to enhance the security and accuracy of intrusion detection systems. The data from the blockchain is selected using a Greedy-based genetic algorithm and then split into training and testing datasets. This method ensures that the data remains immutable and comprehensive, providing a robust foundation for training the deep learning classifier to predict attacks.

The simulations aimed to evaluate the model's ability to accurately and securely classify data into categories. The results demonstrated that our proposed method significantly improves classification precision and enhances data security. By utilizing the cryptographic structure of the blockchain and the RSA hashing algorithm, we ensured that the data blocks are securely created and verified. The encrypted data is then used to train and test the model, allowing for accurate and reliable intrusion detection.

Furthermore, the validated model can use the deep learning classifier to analyze detected attacks and determine their origins. The goal of the simulation was to assess the accuracy and precision of the model's classifications, and the results confirmed that our approach not only improves classification accuracy but also strengthens data security.

As a future direction, we aim to expand the scope of this work to include the practical implementation of the proposed system and evaluate its performance under real-time constraints. This will involve testing the system in real-world scenarios to ensure its effectiveness and scalability in dynamic and diverse net- work environments.

8. References

1. Afanasev MY, Fedosov YV, Krylova AA, Shorokhov SA. An application of blockchain and smart contracts for machine-to-machine communications in cyber-physical production systems. In: Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS); 2018 May 15-18; St. Petersburg, Russia. IEEE; 2018. p. 13-9. doi: 10.1109/ICPHYS.2018.8387630
2. Aljabri F, Jemili F, Korbaa O. Convolutional neural network for intrusion detection using blockchain technology. Int J Comput Appl. 2023;46(2):67-77. doi: 10.1080/1206212X.2023.2284443
3. Aljabri F, Jemili F, Korbaa O. Intrusion detection in cyber-physical system using RSA blockchain technology. Multimed Tools Appl. 2024;83:48119-40. doi: 10.1007/s11042-023-17576-z
4. Alkadi O, Moustafa N, Turnbull B. A collaborative intrusion detection system using deep blockchain framework for securing cloud networks. In: Proceedings of the SAI Intelligent Systems Conference; 2020. Cham: Springer; 2020. p. 553-65. doi: 10.1007/978-3-030-29516-5_40
5. Almajed R, Ibrahim A, Abualkishik AZ, Mourad N, Almansour FA. Using machine learning algorithm for detection of cyber-attacks in cyber physical systems. Period Eng Nat Sci. 2022;10(3):261-75. doi: 10.21533/pen.v10i3.2673
6. Bouachir O, Aloqaily M, Tseng L, Boukerche A. Blockchain and fog computing for cyberphysical systems: the case of smart industry. Computer. 2020;53(9):36-45. doi: 10.1109/MC.2020.2992743
7. Chang V. Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification. Comput Electr Eng. 2021;92:107186. doi: 10.1016/j.compeleceng.2021.107186
8. da Silva TAF, Barros GB, Carvalho TCMB. A blockchain-based intrusion detection system for smart grids. In: Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS); 2017. Porto, Portugal.
9. Evsutin O, Melman A, Abd El-Latif AA. Overview of information hiding algorithms for ensuring security in IoT based cyber-physical systems. In: Security and Privacy Preserving for IoT and 5G Networks. Cham: Springer; 2022. p. 81-115.
10. Gao Y. A novel semi-supervised learning approach for network intrusion detection on cloud-based robotic system. IEEE Access. 2018;6:50927-38. doi: 10.1109/ACCESS.2018.2869962
11. Hajimirzaei S, Navimipour NJ. Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. ICT Express. 2019;5(1):56-9. doi: 10.1016/j.icte.2018.09.003
12. Hannah S. Blockchain-based deep learning to process IoT data acquisition in cognitive data. Biomed Res Int. 2022;2022:5038851. doi: 10.1155/2022/5038851
13. Hasan A. A blockchain-based approach for intrusion detection in wireless sensor networks. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS); 2018.
14. Jemili F. Intelligent intrusion detection based on fuzzy big data classification. Cluster Comput. 2022. doi: 10.1007/s10586-022-03769
15. Kariri E. IoT powered agricultural cyber-physical system: security issue assessment. IETE J Res. 2022:1-11. doi: 10.1080/03772063.2022.2032848
16. Karuppusamy L. Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy. Int J Numer Model Electron Networks Devices Fields. 2022;35(1):e2948. doi: 10.1002/jnm.2948
17. Khalil A. A literature review on blockchain-enabled security and operation of cyber-physical systems. In: Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC); 2022 Jun 27-Jul 1; Turin, Italy. IEEE; 2022. p. 1774-9. doi: 10.1109/COMPSAC54230.2022.00234
18. Khan R. Security and privacy in connected vehicle cyber physical system using zero knowledge succinct non interactive argument of knowledge over blockchain. Appl Sci. 2023;13(3):1959. doi: 10.3390/app13031959
19. Krishnaveni S. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. Cluster Comput. 2021;24(3):1761-79. doi: 10.1007/s10586-020-03222-y
20. Mishra P, Varadharajan V, Pilli ES, Tupakula U. VMGuard: a VMI-based security architecture for intrusion detection in cloud environment. IEEE Trans Cloud Comput. 2018;8(3):957-71. doi: 10.1109/TCC.2018.2800199
21. Samad K, Hasan M, Islam R. A blockchain-based intrusion detection system for healthcare 4.0. J Ambient Intell Humaniz Comput. 2020;11(4):1783-97. doi: 10.1007/s12652-019-01431-2
22. Trivedi RS, Patel SJ. Security and privacy aspects in the internet of things (IoT) and cyber-physical systems (CPS). In: Handbook of Research on Internet of Things and Cyber-Physical Systems. Palm Bay (FL): Apple Academic Press; 2022. p. 453-90.
23. Wang J, Zhao N, Song B, Lin P, Yu FR. Resource management for secure computation offloading in softwarized cyber-physical systems. IEEE Internet Things J. 2021;8(11):9294-304. doi: 10.1109/JIOT.2021.3060802
24. Yuvaraj N. Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking. Math Probl Eng. 2021;2021:6644652. doi: 10.1155/2021/6644652
25. Zhao Y, Li Y, Mu Q, Yang B, Yu Y. Secure pub-sub: blockchain-based fair payment with reputation for reliable cyber physical systems. IEEE Access. 2018;6:12295-303. doi: 10.1109/ACCESS.2018.2801234