[1] **Nitu Sharma**

[2] **Dr.Ramesh Vishwakarma**

# Real-Time Cross Data Auto Evaluation System for Enhancing Security and Privacy in the Internet of Things

Journal of Electrical Systems

***Abstract*** -Even though the rapid expansion of the Internet of Things (IoT) has led to significant advancements in a number of industries, security and privacy are still top priorities. Traditional security solutions are often ineffective due to the diversity of IoT devices and their resource limitations. This research proposes the Real-Time Cross-Data Auto Evaluation System (RTCDAES) to enhance security and privacy in IoT ecosystems. The solution swiftly detects and removes security threats by utilizing cross-data analysis from several IoT devices. Furthermore, the RTCDAES ensures privacy protection by implementing secure data signal transmission and storage techniques and lowering the likelihood of data leakage and unauthorized access. The proposed system significantly improves the overall security posture of IoT networks, provides a scalable and dependable solution for real-world applications, and demonstrates high accuracy and efficiency in threat detection.

***Keywords:*** IoT**,** Remote Device Authentication, Cross Data Auto Evaluation.

## INTRODUCTION

In the quickly developing IoT paradigm, wearable technology, smart sensors, RFID tags, and smartphones connect physical objects with the digital world. Thanks to this integration, physical objects can now function over the Internet to gather and share data about the physical environment. Numerous major security and privacy risks arise from the large range of cyber-enabled products operating remotely over different networks and protocols. Physical assaults and attacks on the semantic application layers, which process and interpret data, are examples of security concerns. One major issue is that most IoT devices run on low energy and have little computational power, necessitating the use of straightforward security solutions. Because of the stringent memory and processing requirements of its devices, the majority of sophisticated security solutions, including firewalls, secure protocols, and conventional cryptography, cannot be easily applied to IoT.

Creating secure IoT designs and creating lightweight security methods have been the two main focuses of IoT security research in the past. Efficient object authentication in IoT systems is challenging due to the limited processing capability of IoT objects. The researcher focused on anonymous entity authentication and proposed a straightforward method for Internet of Things applications. By employing a dynamic accumulator for credentials, their proposed method solved the issue of credentials updating, which requires processing resources from IoT devices. In order to create secure IoT designs, the researchers proposed a secure communication architecture specifically designed for cloud-connected IoT objects.

In their suggested design, they have incorporated end-to-end encrypted connectivity between low-power Internet of Things devices and cloud back-ends. The researchers proposed a different architecture for IoT object security that shifts the computations needed for authentication to the cloud in order to lessen the strain on IoT devices. One potential method for securing wireless devices on IoT nodes with little to no computational work is to analyse IoT signals.

## REMOTE DEVICE AUTHENTICATION IN THE IoT

As the Internet of Things (IoT) expands, protecting the vast number of connected devices becomes increasingly important. "Remote Device Authentication in the IoT" examines the critical need for robust authentication protocols to ensure the security and integrity of IoT networks. A trustworthy environment must be created for a range of devices, from home appliances to industrial sensors, in order to prevent malicious assaults, illegal access, and data breaches. With an emphasis on low-power protocols and cryptographic algorithms suitable for

[1] Research scholar (PhD), Rabindranath Tagore University Bhopal(MP), India, nitutct@gmail.com

[2] Dept. Computer science, Rabindranath Tagore, University Bhopal, India ,rameshaisect@gmail.com

devices with constrained resources, this paper investigates a variety of authentication techniques created for Internet of Things networks.

The research project examines more traditional methods like password-based systems and their shortcomings in the context of the Internet of Things, in addition to more advanced approaches like public key infrastructure (PKI), biometrics, and RDSLBT-based solutions. Additionally, it addresses the challenges of scalability, interoperability, and managing diverse authentication needs across diverse IoT devices. This study finds new trends and best practices that enhance device authentication without sacrificing system effectiveness or user convenience by analysing experimental work and real-world implementations.

To ensure that distant IoT devices can interact safely and dependably in a world where connectivity is growing, the goal is to offer complete security in the rapidly changing IoT landscape and to suggest solutions that strike a balance between robustness and feasibility.

Remote device authentication is a vital component in the rapidly evolving field of the Internet of Things and networked digital environments. The proliferation of smart devices, ranging from industrial sensors to gadgets, highlights the need for secure and reliable communication between them. Remote device authentication involves verifying the identification of a device attempting to connect to a network or another device to stop unwanted access and safeguard critical data.

**Algorithm: Cross Data Auto Evaluation Remote Device Load Balancing**

*Step 1: Initialization*

1. **Define Parameters:**

- devices: List of remote devices.
- data_sources: List of data sources to be processed.
- load_threshold: Maximum load per device.
- evaluation_metrics: Criteria for evaluating data processing effectiveness.

2. **Initialize Device States:**

- For each device in devices:
  - Set current_load to 0.
  - Set data_processed to 0.

*Step 2: Data Evaluation*

1. **Collect Data Metrics:**

- For each data source in data_sources:
  - Evaluate the data characteristics (e.g., size, complexity).
  - Assign a priority score based on predefined metrics (e.g., urgency, importance).

2. **Sort Data Sources:**

- Sort data_sources based on the priority score in descending order.

*Step 3: Load Balancing*

1. **Distribute Data Sources:**

- For each data source in the sorted list:
  - Identify the device with the least current_load that is below the load_threshold.
  - If such a device exists:
    - Assign the data source to the device.
    - Update device.current_load by adding the data source's load.

- Increment device.data_processed.

2. **Reevaluate Load:**

- After assignment, check each device:
  - If current_load exceeds load_threshold, flag the device for reallocation.

*Step 4: Reallocation (if needed)*

1. **Identify Overloaded Devices:**

- For each device:
  - If current_load exceeds load_threshold, mark it as overloaded.

2. **Reassign Data:**

- For each overloaded device:
  - Identify excess data that can be offloaded.
  - Reassign excess data to the least loaded available device.

*Step 5: Monitoring and Reporting*

1. **Monitor Device Status:**

- Continuously monitor the load and performance metrics of each device.
- Adjust assignments dynamically based on real-time performance data.

2. **Generate Reports:**

- Create periodic reports summarizing:
  - Total data processed.
  - Device loads.
  - Any reallocations that occurred.

*Step 6: End of Cycle*

1. **Evaluate Effectiveness:**

- At the end of a processing cycle, evaluate:
  - Load distribution efficiency.
  - Data processing effectiveness based on evaluation metrics.

2. **Adjust Parameters:**

- Adjust load_threshold and evaluation_metrics based on performance data to improve future iterations.

## RESULTS ANALYSIS

The CDAERDLB mode is compared with the following algorithms as sine-cosine algorithm (SCA) (Mirjalili, 2016), salp swarm algorithm (SSA) (Mirjalili et al., 2017), Jaya algorithm (JA) (Rao, 2016), Bat algorithm (BA) (Yang, 2010), and grey wolf optimization algorithm (GWO) (Mirjalili et al., 2014), PSO, used for the feature selection. .

| | **CAS-SSA** | **PSO** | **SCA** | **SSA** | **JA** | **BA** | **GWO** |
|---|---|---|---|---|---|---|---|
| **KNN** | 83.3 | 82.7 | 82.95 | 82.7 | 82.95 | 82.6 | 82.3 |
| **XGBoosT** | 84.75 | 84 | 84.2 | 84.15 | 83.95 | 83.9 | 84.1 |
| **CDAERDLB** | 85.80 | 85.03 | 85.25 | 85.19 | 84.99 | 85.01 | 85.21 |

Table 1 – Accuracy

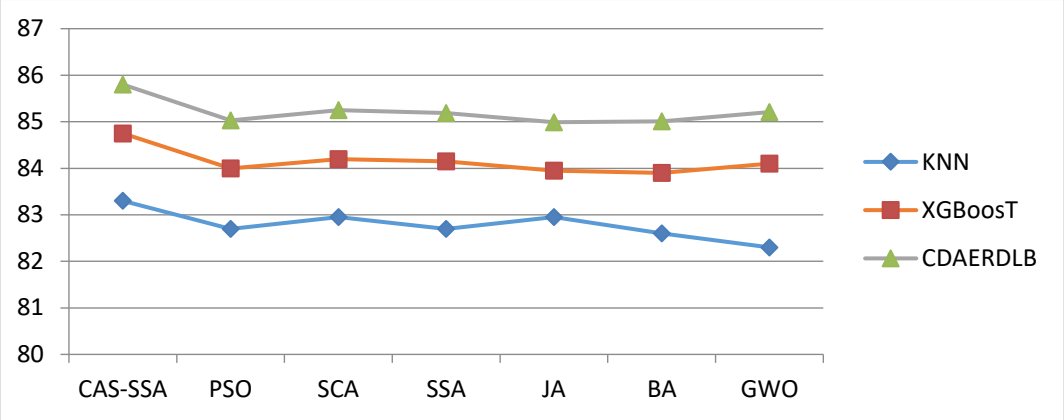


Fig 1 –Accuracy

XGBoost classifier. On the other side, BA attains an accuracy of 82.6% with KNN 83.9% with the XGBoost classifier. CDAERDLB. On the other side, BA attains the minimum accuracy of 85.01% with CDAERDLB, which is the highest among all other methods.

| | CAS-SSA | PSO | SCA | SSA | JA | BA | GWO |
|---|---|---|---|---|---|---|---|
| **KNN** | 84 | 83 | 84 | 83 | 83 | 83 | 83 |
| **XGBoosT** | 86 | 85 | 85 | 85 | 85 | 85 | 85 |
| **CDAERDLB** | 88 | 86 | 86 | 86 | 86 | 86 | 86 |

Table .2 –Precision

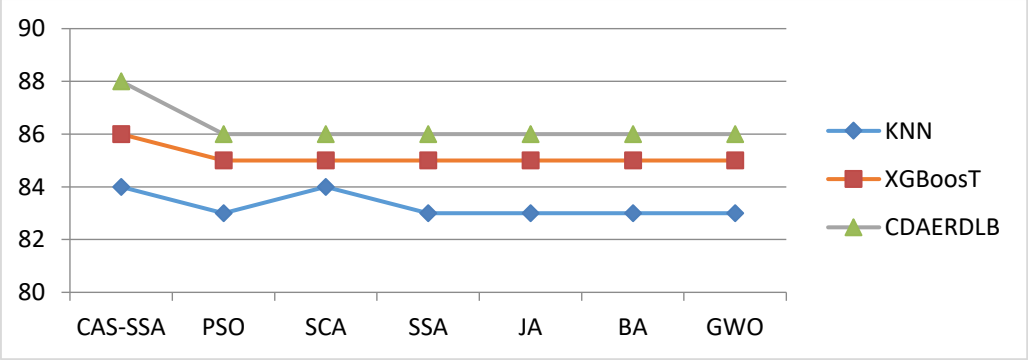


Fig .2 –Precision

| | CAS-SSA | PSO | SCA | SSA | JA | BA | GWO |
|---|---|---|---|---|---|---|---|
| **KNN** | 83 | 83 | 83 | 83 | 83 | 83 | 82 |
| **XGBoosT** | 85 | 84 | 85 | 84 | 84 | 84 | 84 |
| **CDAERDLB** | 87 | 86 | 86 | 85 | 85 | 85 | 85 |

Table .3 Recall.

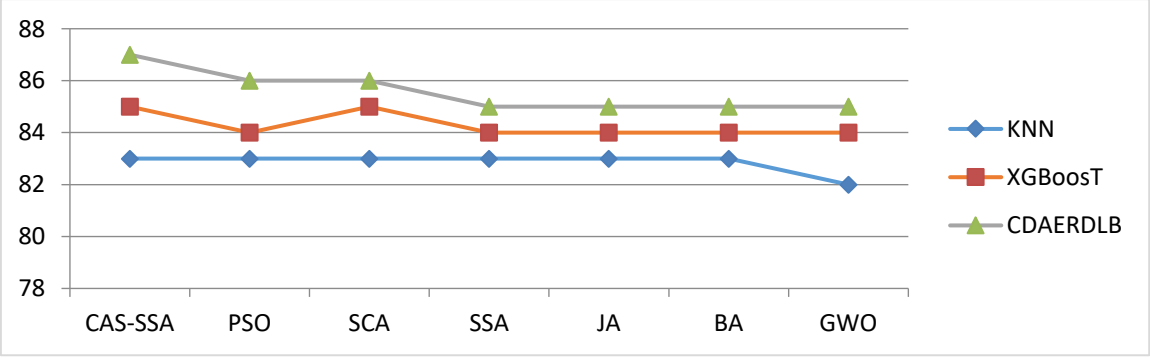


Fig. .3 Recall

| | CAS-SSA | PSO | SCA | SSA | JA | BA | GWO |
|---|---|---|---|---|---|---|---|
| **KNN** | 83 | 83 | 83 | 83 | 83 | 83 | 82 |
| **XGBoosT** | 85 | 84 | 85 | 84 | 84 | 84 | 84 |
| **CDAERDLB** | 87.49714 | 86 | 86 | 85.49708 | 85.49708 | 85.49708 | 85.49708 |

Tabl .4 F-score


Fig .4 F-score

Similarly, recall and F-Score of SCA-SSA are highest among other methods with CDAERDLB as shown in Figures .3, and 4, respectively.

| | CAS-SSA | PSO | SCA | SSA | JA | BA | GWO |
|---|---|---|---|---|---|---|---|
| **KNN** | 145.75 | 217.71 | 152.9 | 216.85 | 215.07 | 210.44 | 213.59 |
| **XGBoosT** | 96.42 | 233.96 | 137.79 | 25.77 | 228.4 | 239.45 | 290.02 |
| **CDAERDLB** | 96.32 | 232 | 136.36 | 25.33 | 2226.01 | 239.22 | 288.06 |

Table .5 Time

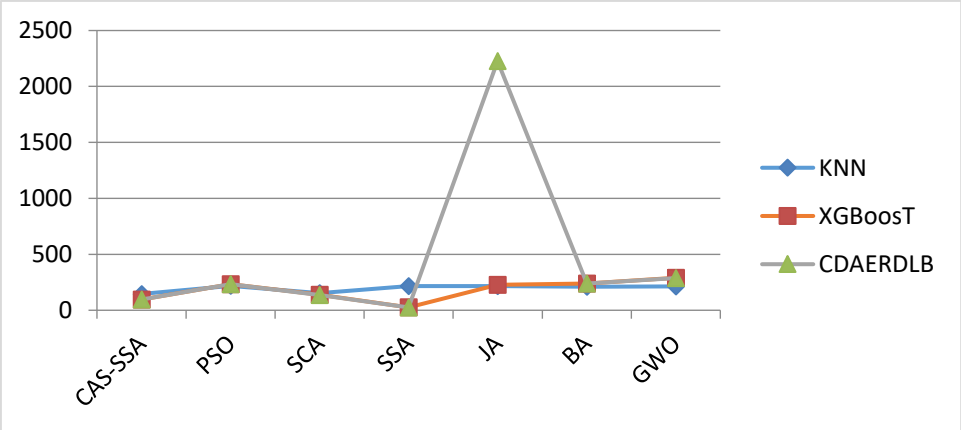


Fig. .5 Time

SCA-SSA takes the lowest execution time of 96.32 s with CDAERDLB, and 96.42 s with XGBoost as depicted in Figure 5.

It is essential to protect IoT devices from malicious activity. These smart gadgets generate heterogeneous data. To decrease data quantity and detection time without sacrificing system accuracy, a CDAERDLB with an

effective feature selection approach is crucial. The suggested work's performance is assessed using the IoTID20 dataset. A hybridized SCASSA algorithm is used to choose the closest device based on pre-processed data. The intrusive data is then multiclass classified using the CDAERDLB methodology. The outcome of the experiment indicates that the suggested technique improves upon previous comparable methods. As a result, CDAERDLB achieves great accuracy in the shortest amount of time during execution.

## CONCLUSION

While the rapid proliferation of IoT devices has undeniably transformed various sectors by enhancing efficiency and connectivity, the pressing issues of security and privacy cannot be overlooked. Traditional security measures often fall short in addressing the unique challenges posed by the diverse and resource-constrained nature of IoT ecosystems. The proposed Real-Time Cross-Data Auto Evaluation System (RTCDAES) emerges as a promising solution, leveraging cross-data analysis to swiftly detect and mitigate security threats. By implementing robust data transmission and storage protocols, RTCDAES not only fortifies security but also protects user privacy against potential breaches. This innovative approach not only offers a scalable and reliable framework for IoT applications but also significantly elevates the overall security landscape. As we continue to integrate IoT technologies into our daily lives, prioritizing advanced security solutions like RTCDAES will be essential to ensuring a safe and trusted digital environment.

## REFERENCES

1. A. Khraisat and A. Alazab, “A critical review of intrusion detection systems in the Internet of Things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges”, Cyber Security 4(18), 2021, DOI: 10.1186/s42400-021-00077-7.
2. E. C. Ugwuabonyi and E.Z. Orji, “Issues and Challenges in Security and Privacy of Internet of Things (IoT)”, International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS), 7(12), 2018, ISSN 2278-2540.
3. T. A. Tchakoucht and M. Ezziyyani, “Building A Fast IntrusionDetection System For High-Speed Networks: Probe and DoS Attacks Detection”, Procedia Computer Science, 127, pp. 521–530, 2018.
4. J. Deogirikar and A. Vidhate, “Security Attacks in IoT: A Survey.International Conference on IoT in Social, Mobile, Analytical and Cloud”, I-SMAC- 2017, IEEE, 2017.
5. O. Alkadi, N. Moustafa, B. Turnbull and K. R. Choo, “A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks”, IEEE Internet of Things Journal, 2020, DOI:10.1109/JIOT.2020.2996590.
6. Rishi Kumar Sharma,“An Internet of Data Center Robotic Things for Cloud Robotics: A Concept of Data Center for a Green Environment”, JST , 2024.
7. Rishi Kumar Sharma,"Prospects and Potential Impacts of Cloud Robotics In Improving Agricultural Farm Produce: A Case of India" ,IJIEMR, 2024.