

Novel intelligent trust computation for securing internet-of-things using probability based artificial intelligence

Nasreen Fathima¹, Mysore Shantharaj Sunitha Patel², Kiran Basavegowda³

¹Department of Computer Science and Design, Academy for Technical and Management Excellence (ATME) College of Engineering, Mysuru, India

²Department of Computer Science and Engineering-Artificial Intelligence and Machine Learning, ATME College of Engineering, Mysuru, India

³Department of Computer Science and Engineering, PES University, Bangalore, India

Article Info

Article history:

Received Apr 4, 2024

Revised Oct 30, 2024

Accepted Nov 11, 2024

Keywords:

Artificial intelligence

Cryptography

Internet-of-things

Probability

Reinforcement learning

Security

ABSTRACT

With rising demands of smart appliances with normal locations transforming themselves in smart cities, internet-of-things (IoT) encounters various evolving security challenges. The frequently adopted encryption-based approaches have its own limitation of identifying dynamic threats while artificial intelligence (AI) based methodologies are found to address this gap and yet they too have shortcomings. This manuscript presents an intelligent trust computational scheme by harnessing probability-based modelling and AI-scheme for monitoring the dynamic malicious behavior of an unknown adversaries. The study contributes towards a novel AI-model using reinforcement learning towards leveraging decision making for confirming the presence of unknown adversaries. The benchmarked study shows that proposed system offers significant improvement when compared to existing AI-models and other cryptographic schemes with respect to delay, throughput, detection accuracy, execution duration.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Nasreen Fathima

Department of Computer Science and Design

Academy for Technical and Management Excellence (ATME) College of Engineering

Bannur Rd, Mysuru, Karnataka 570028, India

Email: nasreenfathima16@gmail.com

1. INTRODUCTION

In large-scale internet-of-things (IoT) deployments, security concerns become even more pronounced due to the sheer volume of devices, data, and potential attack vectors. With a large number of interconnected devices, there are more entry points for attackers to exploit. Each device represents a potential target, increasing the overall attack surface and making it more challenging to defend against cyber threats [1]. Large-scale IoT deployments are susceptible to distributed denial-of-service (DDoS) attacks, where a massive number of compromised devices overwhelm network infrastructure or targeted systems with traffic. Botnets comprised of IoT devices can amplify the impact of DDoS attacks, causing widespread disruption [2]. Large-scale IoT deployments generate vast amounts of sensitive data, including personal information, location data, and operational data. Ensuring the privacy and protection of this data is paramount to prevent unauthorized access, data breaches, and misuse [3]. Apart from this, implementing security measures at scale across thousands or even millions of IoT devices can be challenging. Ensuring that security protocols, encryption mechanisms, and access controls are consistently applied and updated across the entire deployment requires robust management and automation capabilities [4]. Managing a large number of IoT devices throughout their lifecycle, including provisioning, configuration, monitoring, and decommissioning,

presents security challenges. Ensuring that devices are securely onboarded, regularly patched, and securely retired to prevent them from becoming security liabilities is crucial [5]. Segregating IoT devices into separate network segments based on their function, sensitivity, or trust level can help contain security breaches and limit the impact of compromised devices. However, managing network segmentation at scale and ensuring proper isolation between segments require careful planning and configuration [6]. Many IoT devices in large-scale deployments operate with limited resources, including processing power, memory, and energy. Implementing robust security measures without imposing significant overhead on these resource-constrained devices is a major challenge [7].

Artificial intelligence (AI) can play a significant role in enhancing the security of IoT systems in several ways. AI algorithms can analyze vast amounts of data generated by IoT devices to detect abnormal patterns or behavior that may indicate a security breach. By learning what constitutes normal behavior for devices and networks, AI can identify deviations and potential security threats in real-time, enabling proactive threat mitigation [8]. AI-powered behavioral analysis can identify suspicious activities or unauthorized access attempts within IoT networks. By continuously monitoring device interactions and user behaviors, AI algorithms can detect anomalies indicative of malicious activities, such as unauthorized device access or unusual data transfers [9]. AI-enabled predictive maintenance techniques can help identify security vulnerabilities and weaknesses in IoT devices before they are exploited by attackers. By analyzing device performance data and detecting patterns indicative of impending failures or security breaches, AI can enable proactive remediation actions to mitigate risks and enhance overall system security [10]. Apart from this, it can be also used for cyber threat intelligence [11], adaptive authentication [12], network traffic analysis [13], security automation [14]. However, there are various challenges associated with adopting AI-based model for IoT security viz: i) scalable security performance is quite difficult in large and complex IoT environment, ii) offering uniform and consistent security performance in presence of heterogeneous IoT devices, iii) offering assurance towards optimal security in presence of dynamic environment is the the most challenging issue for existing AI-models, iv) majority of the AI models are highly iterative in operation and demands extensive resources to actually implement them on real-world applications, v) existing AI models are known to offer higher predictive accuracy but less towards computational efficiency.

The related work carried out in this perspective of IoT security are as follows: existing system has witnessed proliferated usage of machine learning (ML) approach towards IoT security. The adoption of support vector machine has been seen in work of Ioannou and Vassiliou [15] where the prime notion is towards classification of network-related attacks. Kaushik *et al.* [16] have used Naïve Bayesian approach to perform classification. Adoption of decision tree is witnessed in work of Alabdulkarim *et al.* [17] to incorporate privacy preservation in healthcare sector. Further, random forest has been proven to offer an effective detection of malwares present in IoT networks as seen in work of Atitallah *et al.* [18]. From the perspective of deep learning (DL) methods, various security schemes have been evolved. Velinchko *et al.* [19] have advocated the usage of artificial neural network towards varied application in IoT. Convolution neural network has been implemented by Alabsi *et al.* [20] towards detection the attack with its extracted features in IoT network. Sayegh *et al.* [21] have used long short-term memory towards improving the intrusion detection in IoT networks assessed with publicly available dataset. Chu and Lin [22] have used generative adversarial network (GAN) in order to enhance the classification of an IoT adversaries while usage of reinforcement learning (RL) has been used for enhancing security as noted in work of Hu *et al.* [23]. Further, hybrid learning approaches have also been used in order to integrate both machine and DL approaches for improving network security in IoT as noted in work of Sagu *et al.* [24], Vu *et al.* [25], and Yaras and Dener [26]. Apart from AI-based model, there are various cryptography-based study models focusing on IoT security. Adoption of advanced encryption standard (AES) is witnessed in work of Rekeraho *et al.* [27] and Hameedi and Bayat [28] towards securing energy monitoring system. Adoption of elliptical curve cryptography (ECC) is seen in work of Matteo *et al.* [29] where a processor has been designed in order to secure communication in IoT applications. Digital signature (DS) has also been extensive used towards authentication in IoT as seen in work of Burgos and Pustisek [30]. Existing study has also noted usage of homomorphic encryption (HE) as presented in work of Albakri *et al.* [31] for facilitating higher secure-enabled communication in IoT groups.

The contribution of the proposed study is a novel computationally intelligent trust computational mechanism harnessing probability modelling and AI methodology for diagnosing lethal threats in IoT. The value added contribution of the study are as follows: i) the study presents a novel smart city region-based study model for monitoring the malicious behavior of unknown threats, ii) the study presents a unique role modelling of IoT devices for facilitating formation of an adversary of novel form that is unknown to system, iii) a novel and simplified probability-based trust computation is carried out on the basis of assigned executional role of each nodes, iv) a new empirical approaches of allocation of reward and penalty is designed for promoting secure data transmission for each participating nodes, and v) RL is applied in order to

leverage an effective decision making for detecting the confirmation of an adversary in IoT networks. The next section presents discussion of adopted research methodology.

2. METHOD

The proposed study model is an extension of our prior research model that has used a unique signature design for enhancing secure authentication in IoT [32], [33]. The primary strength of this part of modelling is the unique and lightweight design of cryptographic model; however, there is still a larger scope of optimizing the computational efficiency as well as security features associated with this model. Therefore, the proposed system revises this implementation model by representing it as a baseline architecture and further introducing a novel intelligent approach to strengthen its security features. For this purpose, the proposed system introduces a novel study model which is a mix of probability-based notion and AI. The architectural diagram of the proposed design is as shown in Figure 1.

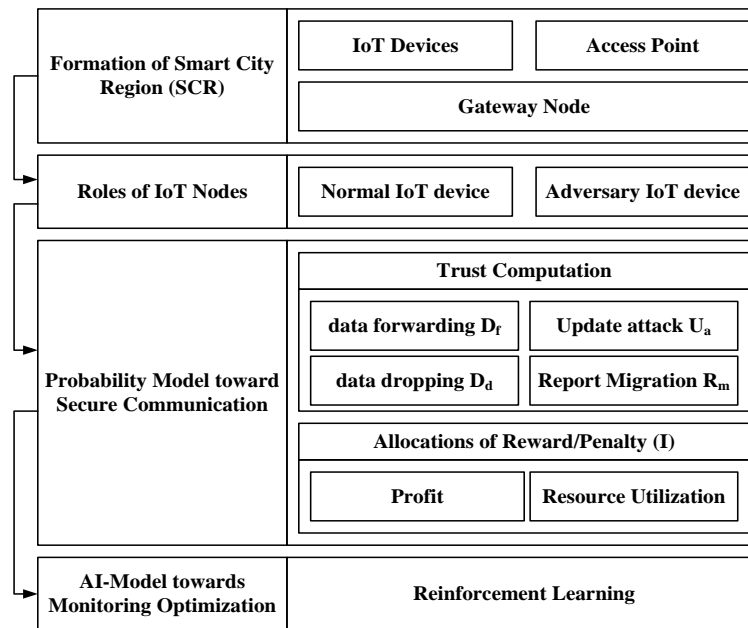


Figure 1. Architecture of proposed study model

The core operation carried out by the essential modules exhibited in Figure 1 are as follows:

- a. Formation of smart city region (SCR): the proposed system constructs a simulation area mapped with one smart city, which is further classified into smaller regions. The study constructs a topology where each smaller region consists of one access point and set of unique operating IoT devices of same type. It will mean that each SCR will represents an individual homogeneous network supported by respective access point. The complete smart city can be now seen in the form of a heterogeneous network. It should be noted that all the access points are further synced with a gateway node to carry out translational services. From Figure 1, it can be understood that it is feasible for one IoT device to join or leave SCR while all the devices within SCR are authenticated using signature scheme by the access point deploying prior model [32], [33].
- b. Roles of IoT nodes: the proposed system considers that there are three types of IoT devices viz. i) normal devices, ii) devices with defective sensory operation, and iii) adversary. The normal devices are meant for sensing the data and forwarding to the respective access point within its SCR while the access point forwards the aggregated information to the gateway node. The devices with defective sensory operations also performs the similar operation like that of normal IoT devices; however, their normal operations are unpredictable for its sustainable operation. They may choose to violate certain task due to internal circuitry problem within the node. Such types of nodes can exists due to environmental impact or accidental event on deployed geographic regions, which are left unattended. The third type of node i.e., adversary are meant to introduce a malicious program. Different from all existing study model, the

proposed system develops a new adversary model by clubbing together lethal functionalities chosen from all the existing reported malicious activities in IoT.

- c. Probability model toward secure communication: this module is responsible for performing trust computation of the participating IoT devices. The model doesn't utilize any form of cryptographic model for this purpose. Rather, it uses a neighborhood monitoring strategy to construct this probability model. Following are the task performed:
 - Trust computation: prior to understand the mechanism of trust computation, it is essential to understand the operations performed by each IoT devices. The proposed scheme hypothesizes two similar operations being carried out by both normal and adversary devices viz. forwarding data and dropping the data packet. The scheme assigns a unique third operation to distinguish normal from adversary device where the normal node will always propagate the identified adversary device to gateway node via access point while the adversary device will launch a malicious program and evade from being detected by migrating itself from current to different SCR with a new spoofed identity. The probability model is then applied i) to evaluate that the identified device is an adversary and ii) to evaluate that the adversary device will either launch malicious program or it will choose to forward the data of normal device. For this purpose, the scheme considers two parameters viz. parameter for number of identified data forwarding D_f and parameter for identified data dropping D_d . Hence, positive trust can be calculated by computing probability as $D_f / (D_f + D_d)$ while negative trust can be calculated by computing probability as $D_d / (D_f + D_d)$. However, this computation is only valid if $D_f \neq D_d$, which is not always the case. Hence, the scheme computes uncertain trust as $A / (A_1 + A_2)$, where attribute A represents dot product of network coefficient, D_f , and D_d , attribute A_1 represents squared summation of D_f and D_d and attribute A_2 represents summation of D_f and D_d . The contribution of this trust computation is that if the value of this uncertain trust reduces, it gives a higher confirmation that the targeted device is adversary. It should be noted that the system has no predefined information of identity of target node to be normal or adversary.
 - Allocations of reward/penalty: It is to be noted that proposed probability model is designed considering three functions each for normal and adversary node. The functions exhibited by normal node are data forwarding D_f , data dropping D_d , and updating attack information U_a . The functions exhibited by adversary node are data forwarding D_f , data dropping D_d , and region migration R_m . Hence, it can be empirically expressed as:

$$\begin{aligned}
 f(normal) &= (D_f, D_d, U_a) \\
 f(adversary) &= (D_f, D_d, R_m)
 \end{aligned}
 \tag{1}$$

From (1), the first two functional attributes i.e., D_f and D_d are same while the third one i.e., U_a and R_m is useful for detection of the normal and adversary node. Further, the proposed scheme uses two variables called as profit and resources used associated with all these functional attributes. The scheme considers profit for executing R_m as I_1 , profit for executing D_f as I_2 , profit for executing U_a as I_3 . Similarly, resources used for D_d as I_4 , resources for D_f as I_5 , resources for U_a as I_6 , and resources for R_m as I_7 . Further, the scheme considers an outlier detection as I_8 by the normal node. All these variables are initialized while performing simulation. The assignment of reward and penalty is shown in Table 1.

Table 1. Empirical assignment of reward/penalty

Target node is adversary		Target node is normal	
Combination	Reward/penalty	Combination	Reward/penalty
(A, C)	$(I_1 - I_4, -I_1 - I_5)$	(C, C)	$(I_2 - I_5, I_2 - I_5)$
(A, D)	$(-I_4, 0)$	(C, D)	$(-I_5, 0)$
(A, R)	$(I_3 - I_4, I_3 - I_6)$	(C, R)	$(-I_5, -I_8 - I_6)$
(C, C)	$(-I_5, I_2 - I_5)$	(D, C)	$(0, -I_5)$
(C, D)	$(-I_5, 0)$	(D, D)	$(0, 0)$
(C, R)	$(-I_3 - I_5, I_3 - I_6)$	(D, R)	$(0, -I_8 - I_6)$
(F, C)	$(-I_7, -I_5)$	(R, C)	$(-I_8 - I_6, -I_5)$
(F, D)	$(-I_7, 0)$	(R, D)	$(-I_8 - I_6, 0)$
(F, R)	$(-I_7, -I_6)$	(R, R)	$(-I_8 - I_6, -I_8 - I_6)$

- d. AI-model towards monitoring optimization: from the discussion of allocation of reward and penalty, it is noted that specific values are assigned on the basis of undertaken actions by the normal or adversary devices. The condition form for the identification is two i.e., i) increased observation of consistently

reducing uncertain trust values and ii) profit of introducing malicious program is significantly less compared to resource to be assigned for introducing this malicious program. All the observed values of the monitored trust are then subjected to AI model which uses RL for performing dynamic decision making. RL can be applied to attack detection in IoT by training agents to make decisions in dynamic environments, adapting to evolving threats and anomalies. Here's how RL can be used for this purpose:

- Environment modeling: RL agents can be trained to model the environment of IoT devices, including normal behavior patterns, network traffic, and interactions between devices. The agent learns to recognize deviations from expected behavior, which may indicate attacks or anomalies.
- State representation: IoT environments often generate high-dimensional and complex data streams. RL models can learn compact representations of these states, capturing relevant information for attack detection while reducing the dimensionality of the problem.
- Action selection: RL agents choose actions based on their learned policies and the observed states of the environment. In the context of IoT security, actions may include isolating suspicious devices, blocking malicious traffic, or alerting administrators.
- Reward design: designing appropriate reward functions is crucial in RL for attack detection. Rewards can be based on the effectiveness of actions taken by the agent in mitigating attacks, minimizing false positives, or maximizing the detection of true threats.
- Adversarial training: RL agents can be trained in adversarial settings, where they learn to anticipate and defend against attacks by interacting with simulated attackers. This helps the agent to become more robust and adaptive to novel attack strategies.
- Continuous learning: IoT environments are dynamic, with new devices joining and leaving the network, and new attack techniques emerging over time. RL models can continuously learn and adapt to these changes, improving their effectiveness in detecting evolving threats.
- Policy improvement: through repeated interactions with the environment, RL agents can improve their policies over time, learning from past experiences and adjusting their behavior to achieve better attack detection performance.
- Hierarchical RL: hierarchical RL can be used to model complex IoT security systems with multiple levels of abstraction. This allows for efficient learning and decision-making at different layers of the IoT infrastructure, from edge devices to network gateways and cloud servers.

The final outcome of the proposed AI model is a confirmed detection of adversary model, irrespective of any type of attacker in IoT. The scheme can easily perform detection of even a minor degree of anomalies exhibited by an adversary node followed by using its agent model that finally detects the adversary node. Hence, the AI model introduced in this study actually complements the probability model towards confirming the identity of both normal and adversary devices in IoT. The prime contribution of this methodology is towards performing a cost-effective, highly reduced iterative, and faster detection of unknown form of adversaries that is left unaddressed in existing literatures. The next section discusses about the study outcomes.

3. RESULT

This section discusses about the outcome accomplished from the implementation of the methodology illustrated in prior section. The assessment is carried out considering 1,000×1,000 m² simulation area with randomly deployed 500 IoT devices in 9 SCRs. The approach was implemented considering 460 nodes are normal nodes and 40 nodes are adversary nodes without any apriori information about their identities. The scripting has been carried out in MATLAB in normal 64-bit windows machine. The outcome analysis is benchmarked by comparing it with existing AI-models and cryptographic models reportedly used for IoT security. The numerical outcome for the comparison with AI models is as shown in Table 2.

Table 2. Numerical outcomes of AI-models

Approaches	Detection accuracy (%)	Execution duration (s)	Throughput (bps)	Delay(s)
Prop	98.4	0.389	4701.99	0.025
ML	92.5	0.511	3105.77	0.278
DL	93.2	0.509	2982.52	0.109
GAN	92.5	0.455	1994.65	0.0365
RL	89.7	0.898	3761.02	0.592
HA	89.9	1.207	2204.63	0.306

The numerical outcome of Table 2 is accomplished as follows: i) the proposed model Prop is initially executed and its performance metric for detection accuracy, execution duration, throughput, and delay are observed, ii) the same framework is then allowed to be executed by substituting the function for random forest used in proposed system with existing AI-models viz. ML, DL, GAN, RL, and hybrid approach (HA). iii) From the perspective of ML approach, the scheme implements Naive Bayes, support vector machine, random forest, and decision tree, their mean is then extracted for each performance metric and retained within Table 2, iv) from the perspective of DL approach, the scheme uses artificial neural network, convolution neural network, and long short term memory followed by extracting their mean for each performance metric and entered in Table 2, v) GAN and RL approaches are applied in form of standalone method on testbed, vi) HA approach integrates varied combination of ML and DL followed by acquiring their mean values to arrive at final numerical outcomes. The numerical outcome of Table 2 is showcased in Figure 2 with respect to all performance metric. Figure 2(a) exhibits that proposed scheme offers approximately 68% increased detection accuracy, execution duration with 32% of reduced processing time Figure 2(b), throughput with 18% of increased communication performance Figure 2(c), and 97% of reduced delay Figure 2(d). The outcome eventually showcases proposed scheme prop to be significantly better than existing exist scheme.

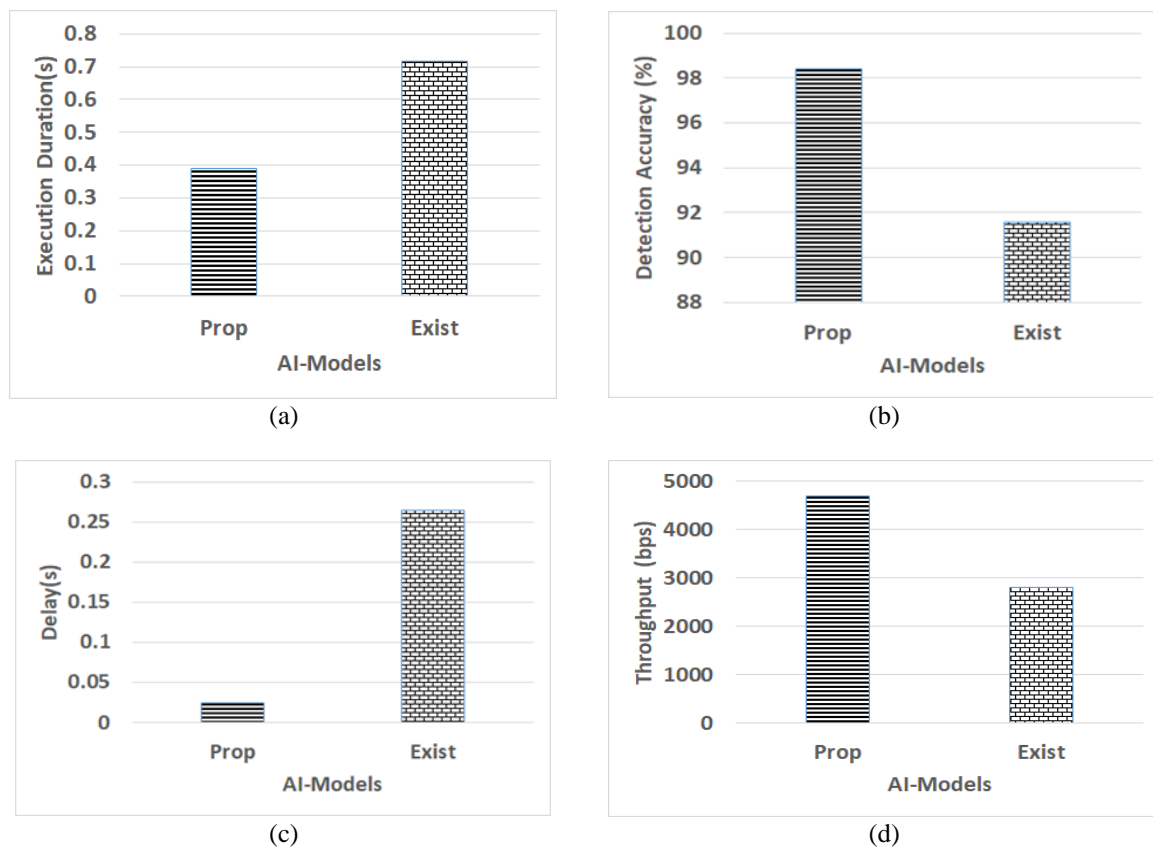


Figure 2. Accomplished outcome for AI-model performance: (a) detection accuracy, (b) execution duration, (c) throughput, and (d) delay

The next line of assessment for proposed system is to perform comparative analysis of proposed system Prop with respect to conventional cryptographic measures viz. AES, ECC, message authentication code (MAC), DS, and HE. Similar strategy as used in analyzing different AI-models is also adopted to analyze various existing cryptographic techniques with proposed scheme to arrive at numerical outcome exhibited in Table 3.

The outcome exhibited in Table 3 is translated to graphical outcome shown in Figure 3 where it can be seen that proposed scheme prop offers approximately 59% of reduced execution time Figure 3(a), 43% of increased throughput Figure 3(b), and 98% of reduced delay in contrast to existing exist cryptographic schemes Figure 3(c). The outcome eventually shows that proposed scheme to be highly cost-effective and

robust performance in contrast to all the prominent cryptographic schemes. It is interesting to be noted that proposed scheme does not uses any form of encryption and yet its performance is potentially good in contrast to frequently adopted encryption techniques in IoT. At the same time, the proposed model doesn't utilize any form of sophisticated or iterative-inclusive scheme which has resulted in faster execution time that supports offering security to practical world applications in IoT.

Table 3. Numerical outcomes of security approaches

Approaches	Execution duration (s)	Throughput (bps)	Delay(s)
Prop	0.389	4701.99	0.105
AES	0.697	3310.66	1.298
ECC	0.589	3497.19	1.782
MAC	0.899	2608.31	3.081
DS	1.466	1501.77	2.551
HE	1.274	1899.68	2.187

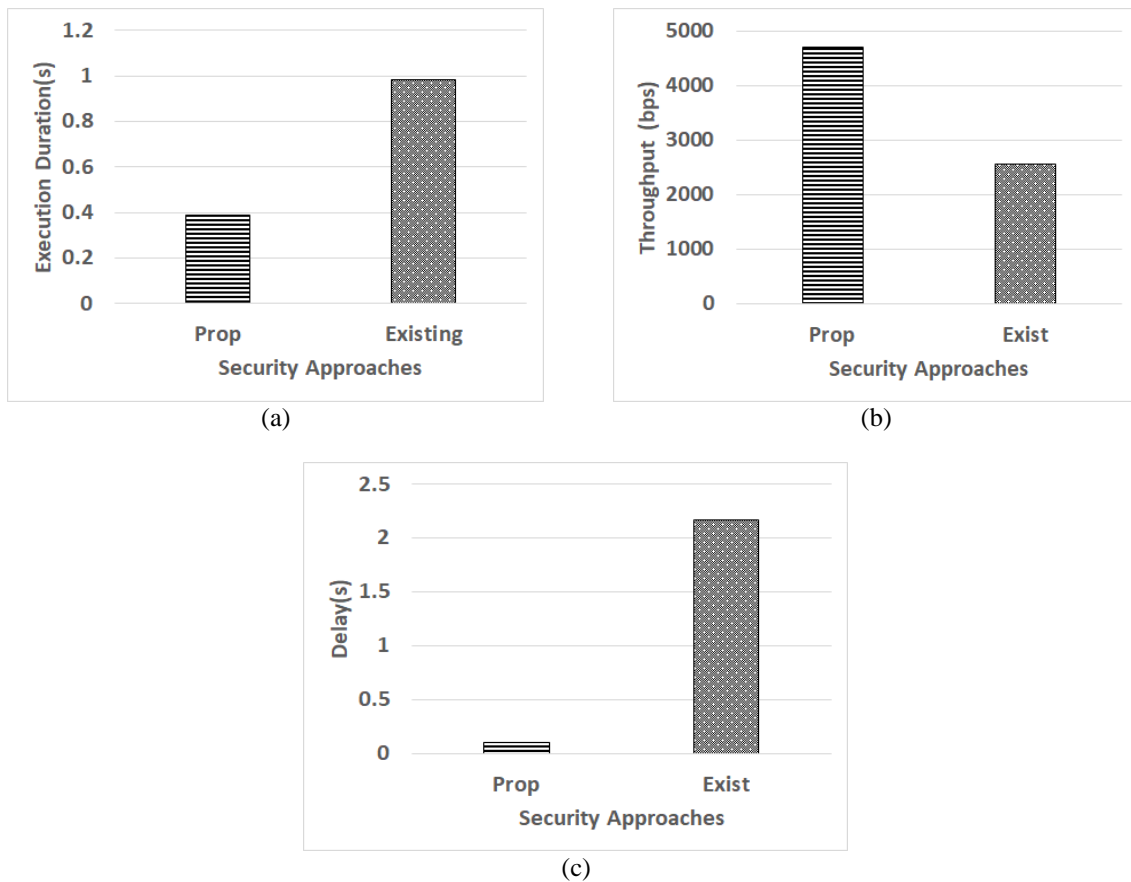


Figure 3. Accomplished outcome for security approaches performance: (a) execution duration, (b) throughput, and (c) delay

Therefore, the outcome presented in Figure 2 and Figure 3 presents the outcome of proposed study in comparison context of previous study towards security approaches. The outcome eventually showcases some of the key findings viz. i) proposed scheme contributes towards 68% accuracy in threat detection which is quite a significant accomplishment in contrast to existing related methods, ii) the response time of proposed scheme is improved to 32% faster, iii) the data delivery performance is noted with 97% minimized delay and 18% enhanced throughput which is dominantly more in contrast to existing AI system, iv) in comparison to encryption-oriented existing solution, proposed scheme is witnessed to exhibit 98% minimized delay, 43% of maximized throughput which is another significant findings. Overall, it is noted that RL approach has potential impact in strengthening the security strength balancing the computational demand and security features.

4. CONCLUSION

This paper has presents a novel security measures that is capable of offering a robust and intelligent trust computation using an integrated probability and AI-based modelling approaches for offering higher degree of resistance from lethal threats in IoT. The proposed study model contributes towards incorporating following novel features: i) the proposed study uses a combination of probability model for intelligent trust computation followed by implementing AI-modelling using RL, ii) the probability-based trust computational model assists in confirming the actual trust scores on the basis of malicious behavior of an adversary, which is more likely to support any form of dynamic networks in IoT, iii) the RL model used in proposed scheme further offers predictive accuracy using its agent-based learning to confirm the presence of adversary in IoT network, iv) the development of proposed model is carried out without any predefined information of identity of adversaries. The proposed research work offers a simplistic guideline towards developing a simplified AI-based security modelling without inclusion of complex internal operation. The future work will be further towards improving the security performance of proposed system with more challenging assessment environment. More optimization approaches will be investigated towards finding correlation between adversary-based events and any events with sub-optimal performance without intrusion. This will assist further to extend the applicability of proposed scheme towards advanced AI-based cyber threats.

ACKNOWLEDGEMENTS

The author expresses gratitude to Academy for Technical & Management Excellence College of Engineering, Mysuru, India for their encouragement and support, and declares that this research was undertaken without financial contributions from any external entities.





REFERENCES

- [1] T. Rajmohan, P. H. Nguyen, and N. Ferry, "A decade of research on patterns and architectures for IoT security," *Cybersecurity*, vol. 5, no. 1, 2022, doi: 10.1186/s42400-021-00104-7.
- [2] S. Dalal *et al.*, "Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00517-4.
- [3] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.
- [4] C. Guo and D. Li, "IoT security privacy protection mechanism and mechanical structure design simulation optimization," *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13634-021-00737-3.
- [5] M. Aaqib, A. Ali, L. Chen, and O. Nibouche, "IoT trust and reputation: a survey and taxonomy," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00416-8.
- [6] D. Mohamed and O. Ismael, "Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00420-y.
- [7] S. Ullah and R. Zahilah, "Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00078-6.
- [8] I. Keshta, "AI-driven IoT for smart health care: security and privacy issues," *Inform. Med. Unlocked*, vol. 30, 2022, doi: 10.1016/j.imu.2022.100903.
- [9] S. M. T. Nizamudeen, "Intelligent intrusion detection framework for multi-clouds – IoT environment using swarm-based deep learning classifier," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00509-4.
- [10] P. Radanliev *et al.*, "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, 2020, doi: 10.1186/s42400-020-00052-8.
- [11] J. Liu *et al.*, "TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network," *Cybersecurity*, vol. 5, no. 1, 2022, doi: 10.1186/s42400-022-00110-3.
- [12] A. Srivastava, S. K. Gupta, M. Najim, N. Sahu, G. Aggarwal, and B. D. Mazumdar, "DSSAM: digitally signed secure acknowledgement method for mobile ad hoc network," *EURASIP J. Wirel. Commun. Netw.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13638-021-01894-7.
- [13] B. Sun, R. Geng, L. Zhang, S. Li, T. Shen, and L. Ma, "Securing 6G-enabled IoT/IoV networks by machine learning and data fusion," *EURASIP J. Wirel. Commun. Netw.*, vol. 2022, no. 1, 2022, doi: 10.1186/s13638-022-02193-5.
- [14] N. Zhou *et al.*, "Container orchestration on HPC systems through Kubernetes," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 10, no. 1, 2021, doi: 10.1186/s13677-021-00231-z.
- [15] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," *J. Sens. Actuator Netw.*, vol. 10, no. 3, p. 58, 2021, doi: 10.3390/jsan10030058.
- [16] K. Kaushik *et al.*, "Multinomial naive Bayesian classifier framework for systematic analysis of smart IoT devices," *Sensors*, vol. 22, no. 19, p. 7318, 2022, doi: 10.3390/s22197318.
- [17] A. Alabdulkarim, M. Al-Rodhaan, T. Ma, and Y. Tian, "PPSDT: a novel privacy-preserving single decision tree algorithm for clinical decision-Support Systems using IoT devices," *Sensors*, vol. 19, no. 1, p. 142, 2019, doi: 10.3390/s19010142.
- [18] S. B. Atitallah, M. Driss, and I. Almomani, "A novel detection and multi-classification approach for IoT-malware using random forest voting of fine-tuning convolutional neural networks," *Sensor*, vol. 22, no. 11, p. 4302, 2022, doi: 10.3390/s22114302.
- [19] A. Velichko, D. Korzun, and A. Meigal, "Artificial neural networks for IoT-enabled smart applications: Recent trends," *Sensors*, vol. 23, no. 10, p. 4853, 2023, doi: 10.3390/s23104853.
- [20] B. Alabsi, M. Anbar, and S. Rihan, "CNN-CNN: Dual convolutional neural network approach for feature selection and attack detection on internet of things networks," *Sensors*, vol. 23, no. 14, p. 6507, 2023, doi: 10.3390/s23146507.
- [21] H. R. Sayegh, W. Dong, and A. M. Al-madani, "Enhanced intrusion detection with LSTM-based model, feature selection, and SMOTE for imbalanced data," *Appl. Sci*, vol. 14, no. 2, p. 479, 2024, doi: 10.3390/app14020479.





- [22] H.-C. Chu and Y.-J. Lin, "Improving the IoT attack classification mechanism with data augmentation for generative adversarial networks," *Appl. Sci.*, vol. 13, no. 23, p. 12592, 2023, doi: 10.3390/app132312592.
- [23] L. Hu, C. Han, X. Wang, H. Zhu, and J. Ouyang, "Security enhancement for deep reinforcement learning-based strategy in energy-efficient wireless sensor networks," *Sensors*, vol. 24, no. 6, p. 1993, 2024, doi: 10.3390/s24061993.
- [24] A. Sagu, N. S. Gill, P. Gulia, J. M. Chatterjee, and I. Priyadarshini, "A hybrid deep learning model with self-improved optimization algorithm for detection of security attacks in IoT environment," *Future Internet*, vol. 14, no. 10, p. 301, 2022, doi: 10.3390/fi14100301.
- [25] V. Q. Vu, M.-Q. Tran, M. Amer, M. Khatiwada, S. S. M. Ghoneim, and M. Elsis, "A practical hybrid IoT architecture with deep learning technique for healthcare and security applications," *Informatio*, vol. 14, no. 7, p. 379, 2023, doi: 10.3390/info14070379.
- [26] S. Yaras and M. Dener, "IoT-based intrusion detection system using new hybrid deep learning algorithm," *Electronic*, vol. 13, no. 6, p. 1053, 2024, doi: 10.3390/electronics13061053.
- [27] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, E. Tuyishime, T. C. Balan, and R. Acheampong, "Enhancing security for IoT-based smart renewable energy remote monitoring systems," *Electronics*, vol. 13, no. 4, p. 756, 2024, doi: 10.3390/electronics13040756.
- [28] S. S. Hameedi and O. Bayat, "Improving IoT data security and integrity using lightweight blockchain dynamic table," *Appl. Sci.*, vol. 12, no. 18, p. 9377, 2022, doi: 10.3390/app12189377.
- [29] S. D. Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, and S. Saponara, "Secure elliptic curve crypto-processor for real-time IoT applications," *Energies*, vol. 14, no. 15, p. 4676, 2021, doi: 10.3390/en14154676.
- [30] J. B. Burgos and M. Pustišek, "Decentralized IoT data authentication with signature aggregation," *Sensors*, vol. 24, no. 3, p. 1037, 2024, doi: 10.3390/s24031037.
- [31] A. Albakri, R. Alshahrani, F. Alharbi, and S. B. Ahamed, "Fully homomorphic encryption with optimal key generation secure group communication in internet of things environment," *Appl. Sci.*, vol. 13, no. 10, p. 6055, 2023, doi: 10.3390/app13106055.
- [32] N. Fathima, R. Banu, and G. F. A. Ahammed, "A signature-based data security and authentication framework for internet of things applications," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 12, no. 3, p. 3298, 2022, doi: 10.11591/ijece.v12i3.pp3298-3308.
- [33] N. Fathima, R. Banu, and G. F. A. Ahammed, "Integrated signing procedure based data transfer security and authentication framework for internet of things applications," *Wirel. Pers. Commun.*, vol. 130, no. 1, pp. 401–420, 2023, doi: 10.1007/s11277-023-10291-w.

BIOGRAPHIES OF AUTHORS







Dr. Nasreen Fathima     obtained her Ph.D. degree from Visvesvaraya Technological University, Belagavi, India, in the year 2022. With a distinguished career spanning 19 years in the field of education, she presently holds the position of associate professor and head of the Department of Computer Science and Design at the Academy for Technical & Management Excellence of Engineering, located in Mysuru, India. Her scholarly pursuits predominantly revolve around the domains of network security and internet of things. She has contributed significantly to the academic discourse with the publication of 5 papers in prestigious international conferences, 11 papers in esteemed international journals, and the acquisition of an Indian patent. She can be contacted at email: nasreenfathima16@gmail.com.



Dr. Mysore Shantharaj Sunitha Patel     obtained her Ph.D. degree from Visvesvaraya Technological University, Belagavi, India, in the year 2023. Dr. Sunitha Patel, with a rich career spanning 18 years in the education sector, currently serves as the associate professor and Department Head of CSE-Artificial Intelligence and Machine Learning at the Academy for Technical and Management Excellence of Engineering in Mysuru, India. Her academic interests are centered on network security, internet of things, artificial intelligence, and machine learning. She has made notable contributions to scholarly discussions, boasting a portfolio that includes 4 papers presented at esteemed international conferences, 11 publications in respected international journals, and the successful publication of two Indian patents. She can be contacted at email: mssunithapatel@gmail.com.



Kiran Basavegowda     is an academicians, completed bachelor's degree from Visvesvaraya Technological University, Belagavi, India, in 2011, and a master's degree from the same university in 2013. With a dedicated career spanning over a decade in the realm of education, he currently holds the position of assistant professor in the Department of Computer Science and Engineering at PES University, situated in Bangalore, India. He is academic interests primarily revolve around cutting-edge fields such as artificial intelligence, machine learning, and programming languages. His profound passion for these areas drives his teaching methodologies inspiring students. He can be contacted at email: ranjankiran03@gmail.com.