Grenze International Journal of Engineering and Technology, June Issue

A Study on usage of Social Media and Home Appliances using Social IoT domain with Artificial Intelligence

Kirthan K M[1] and Rekha K S[2]
[1]Assistant Professor, Department of Computer Science & Engineering, Coorg Institute of Technology, Ponnampet, India
Email: kirthanmadappak@gmail.com
[2]Professor, Department of Computer Science & Engineering, JSS Science & Technology University, Mysuru, India
Email: rekhaks@jssstuniv.in

***Abstract*—Social Internet of Things (SIoT) integration with Social Media (SM) platforms and home appliances aims to address challenges related to network navigability, device discovery, and service composition by enabling IoT objects for human SM interaction. This survey proposes an Artificial Intelligence (AI)-based framework applied to SIoT, designed to identify complex, nonlinear relationships between inputs and outputs to classify trustworthy home appliances and services within the SM context. The data from Social Media and trustworthiness of home appliances are analysed using Machine Learning (ML) techniques. SIoT facilitates more efficient interaction through SM and enhances decision-making automation, improving both the user experience and appliance performance. The performance measures of the ML approach is evaluated, enhancing SM communication and optimizing the performance of connected home appliances within the Social IoT ecosystem.**

***Index Terms*— Artificial Intelligence, Deep Learning, Home Appliances, Machine Learning, Social Internet of Things.**

I. INTRODUCTION

Artificial Intelligence is an essential domain in the fields of finance, health, agriculture, and satellite systems. AI has augmented the performance of Internet of Things (IoT), which is crucial for industries involving the manufacture of various home appliances. IoT is a crucial of smart manufacturing, smart health, smart grids, smart cities, and electric vehicles. In smart city environments, data types are captured and vary widely, including images, sensors, electricity and water consumption, videos, social media (SM), text, etc. End-to-end communication between IoT devices and AI occurs through a global network connecting various devices via internet communication. The advancement of AI and IoT has led to the use of common devices for a range of novel applications and innovations. SIoT methods facilitate efficient communication between humans through SM, enhancing social networking capabilities.

The integration of social networks with IoT faces challenges due to advancements in cellular network innovations and wireless networks, which are based on AI. The main challenges for AI and Social IoT include: Quality of Service (QoS), interpretability, security, and big data analytics, which lead to trust issues for humans when adopting appliances.

Grenze ID: 01.GIJET.12.2.83_21

However, the complexity of big data arises from the connections among multiple IoT objects and data streams, which generate vast amounts of data. The maximum utilization of SIoT for home appliances and SM focuses on automation to improve the efficiency of home gadgets by enhancing performance and maintaining trust with users.

The continuous development of AI agents and automated text generation presents various challenges in home automation. AI-refined content agents now generate text that mimics real human speech, contributing to the rise of SM conversations. Additionally, AI applications help in human sentiment analysis, especially in identifying emotions from SM content, using social IoT-based methods.

II. RELATED WORK

- C.-G. Xiang et al.[1] proposed human machine intelligence in which mechanisms have been incorporated to enhance the support extended by machine when more emphasis is given to human intelligence and in another method support is given by humans for the predictions and decisions taken by the machines. The work also proposes how machine and human intelligence can be combined to obtain high accuracy from models.
- A. Ali-Eldin[2] studied the challenges faced by IoT Devices in social internet of things setup. The device relationships are updated independently which causes problems with security. Hence, two solutions were proposed based on distributed trust computation and clous based machine learning.
- T. A. Butt [3] developed edge intelligence involving only the edge devices to participate in relationship established in social internet of things environment of smart city. The work also shows the maximum model output is obtained with local artificial intelligence processing employed on the local edge devices.
- S. Sagar et al.[4] developed a trust environment for object to object interaction in SIOT environment. In the proposed model complex non-linear relationship between device to device is avoided thereby building a trust environment by considering the past interactions of device. The past interactions was also used to measure the degree of relationship and the Trust SIOT model showed higher performance when evaluated.
- M. Hosseinzadeh et al. [5] mentioned that the highest level of SIOT is yet to be explored and the exploration will result in social networks be creating like human networks. The potential risks of fault tolerance and security in SIOT environment has to be overcome.
- D. Geissler et al.[6] proposed a work in which the sustainability was bought into the machine learning approaches by providing human feedback in loop which provided energy aware machine learning tasks to be carried out.
- M. Cukurova [7] collaborated artificial intelligence role along with human intelligence on analytical learning. The proposed work showcases how hybrid intelligence can be bought into education.
- K. Krinkin et al. [8] developed an alternative approach for making intelligent systems non centric based on human machine hybridization. In this approach primary data drawn from concepts will be enhanced with human inputs involving the concept of human intelligence. The enhanced concept can be evolved further incorporating machine intelligence to learn the hidden features.

A. Usage of SIoT in Social Media

The integration of SIoT in SM platforms enables smarter, context-aware interactions between users and connected devices.

The social data and IoT, together referred to as SIoT improves user experiences through personalized recommendations and enhanced device coordination based on the observed social behaviour and user preferences.

- S. Khan et al. [9] developed a trustworthy environment for relationship changes between devices in a social internet of things environment during context changes. The work also focused on updating relationship between objects for maintaining security.
- S. A. A. Bokhari et al. [10] suggested an Artificial Intelligence (AI) technique to identify the direct relationship between cybersecurity and e-Governance. The use of AI facilitated the role of e-Governance among the moderating effects of cybersecurity and stakeholder's connections on the relationship among e-Governance and AI.

  Stakeholder interest was examined as modelling factor in understanding AI, e-Governance and cybersecurity. However, maintaining trust between IoT devices based on social interactions, user preferences, and device characteristics, was complex due to system reliability issues.

B. Usage of SIoT on Home Appliances

The combination of SIoT in home appliances improves devices by enabling them to interact intelligently based on user preferences and social contexts. SIoT enhances automation, energy efficiency, and personalized experiences, improving the overall functionality and convenience of smart homes.

- N. Imran et al. [11] developed an IoT-based task management system model using a Deep Neural Network-based Particle Swarm Optimization (DNN-PSO) optimizer to solve local minima problems in smart residual buildings through predictive optimization. This system provided both a predictive and an optimization module to address energy consumption reduction issues. The predictive optimization mechanism was utilized for analyzing task duration and energy consumption. The energy management system operated at the task level by providing predictive optimization to guide planning and make decisions, as well as predicted and optimized outcomes. By forecasting residual energy consumption, the system reduced energy costs through predictive analysis. However, the system's performance was constrained by the challenges associated with integrating diverse IoT devices, leading to inefficiencies in communication and data exchange between them.
- S. Fatima et al. [12] made a study on how the Technologies of IoT are evolving and the security related concerns in home automation. It majorly focuses on the face recognition problem of the home environment in which security concerns holds a major role. The study shows how different algorithms can be applied for the face recognition problem to overcome the issues involved in security.
- P. Rajesh et al.[13] developed a model named Sailfish Optimizer Adaptive Neuro-Fuzzy Inference System (SFOANFIS), combining SFO and ANFIS to manage resources and power in the Distribution System(DS). The SFOANFIS method used Internet Protocol(IP) for connectivity with the cloud-based IoT, helping to control smart energy systems in home. IoT-based communication in the DS allowed a centralized server to collect demand response data, which was then managed by the SFOANFIS method to enhance network flexibility and ensure optimal resource utilization. However, the system's reliance on IoT connectivity and centralized data management caused scalability and security issues.
- L. Fang et al.[14] implemented a CNN to pre-process univariate data and transform it into multidimensional features through temporal two-layer convolution operations. The CNN approach involved a hybrid DNN for power forecasting the consumption in individual households, using a K-step forecasting method to predict multiple values simultaneously.

III. EXISTING SYSTEM

The integration of IoT in a social context is challenging due to varying protocols and the complexities of social dynamics, which affect device interactions, leading to unreliable communication across different platforms. Trustworthiness in social media interactions, user preferences, and device characteristics becomes complex due to system instability, which may result in unauthorized attacks. Security challenges arise when managing and processing the large volumes of data forwarded by multiple users from social media interactions, which further complicates the system, leading to inefficient data management. In a Social IoT environment, safeguarding sensitive user data and ensuring secure interaction among devices is challenging due to the dynamic nature of device interconnections, which increases the risk of data breaches and misuse. The number of users and connected devices faces increased scaling difficulties due to the heterogeneous network of devices, which affects user trust, satisfaction, and leads to performance degradation.

From the survey it is understood that relationship update between objects in social internet of things is an important parameter to achieve better functionality, performance and efficiency. The updating of objects can be by the context changes such as temporal, spatial, mobility and socio-network relationship (parental, owner, co-work, social, co-locate). These context changes takes place as per the recommendation of the artificial intelligent model. This model can be personalized using hybrid intelligence to provide recommendations which results in strong intelligent system.

IV. PROPOSED METHODOLOGY

Based on the survey, the proposed methodology creates a recommendation model specifically customized to the unique needs and preferences of users within the environment of SIoT for Home Automation. It merges machine learning algorithms and domain-specific expert systems to ensure the accuracy, relevance, and robustness of recommendations. Deep Q Network algorithm can be applied to achieve machine intelligence. Effective mechanisms for user feedback with a purpose to ensure optimal satisfaction of the user will be defined. Human Intelligence will be provided through a continuous feedback incorporated through a user interface. Hence, the recommendation for the Home Automation Environment will be through the symbiosis of machine intelligence and human intelligence. The proposed models architecture is shown in Fig 1.

A. Algorithm of the Proposed Work

Step 1: Start
Step 2: Input the sensor generated data/ dataset.
Step 3: Apply machine learning algorithm Deep Q Network to develop a training model.
Step 4: Use the model to make predictions for new instances.
Step 5: Employ human intelligence-based recommendations
for the predicted output developed by the model.
Step 6: If the output of the model and human intelligence employed recommendations matches go to Step 8 else go to Step 7.
Step 7: Collect recommendations of the user as a feedback data and provide it back to re-train the model and iterate through step 4.
Step 8: Output the prediction obtained by the combined intelligence of human and the machine
Step 9: Stop

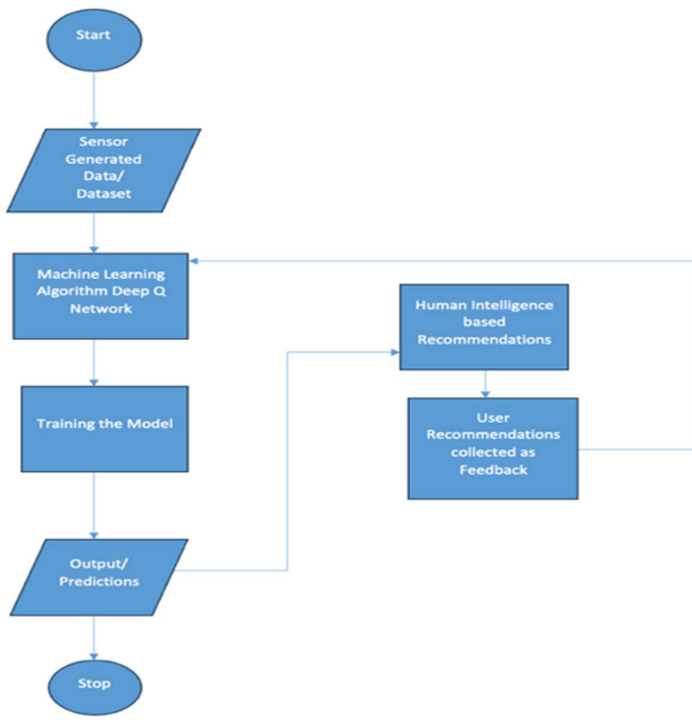

Fig. 1: Proposed Architecture

V. IMPLEMENTATION

A. Prototype Setup

The proposed recommendation model was implemented inside a Smart Home Social Internet of Things (SIoT) environment context. The system is made up of a set of heterogeneous IoT devices including sensors like temperature, humidity, motion, with light intensity too as actuators like smart lights, thermostat, blinds, with appliances. Data generated by sensors is collected by a central controller from a real deployment or simulated dataset. For device interoperability, we use a streamlined middleware system. That middleware enables continuous data acquisition too. A mobile/web-based interface is how it is that the user interacts with the system for allowing of feedback provision and manual intervention in addition to recommendations' visualization. This forms a necessary human-in-the-loop or HITL component for this. It betters the suggested model for advice.

B. Deep Q-Network Design

- The Deep Q-Network (DQN) functions as the machine intelligence module within. The DQN is trained by reinforcement learning principles. The DQN uses the following configurations below.
    - State Space: It shows the contextual environment including sensor values like temperature, occupancy, light levels, and device states.
    - Action Space: Possible actions acting on actuators are defined such as with switching lights both on and off, with adjusting thermostat setpoints, or with controlling blinds. User comfort is balanced via reward function optimization. It does also balance out energy efficiency. Penalties are imposed upon user dissatisfaction or energy wastage, whereas positive rewards are provided when the system ensures user-preferred conditions with minimal energy usage.
    - Training Process: The agent trains whenever it interacts with the environment iteratively through experience replay as well as target network mechanisms so learning may stabilize.

C. Human-in-the-Loop Integration

- The integration of human intelligence ensures the recommendation system adapts coupled with personalizes. The process flow is as follows:

The trained DQN model makes for a recommendation. The recommendation is based upon the current environmental context that it has.

- The user interface displays the recommendation upon validation.
- The user is able to provide some corrected action for rejecting of the recommendation or to accept the recommendation (machine decision confirmed).
- In the event the user rejects at some thing, the system then logs that decision as some feedback data. Afterward, the system adds that feedback data to model retraining.
- That machine intelligence and that human intelligence are symbiotic works to ensure that the system does continuously evolve in order to accommodate user-specific needs.

VI. Results and Discussion

A. Experimental Setup

- The validation for the proposed DQN + Human Feedback Recommendation Model used a smart home simulation framework. The environment consisted of:
    - Devices: 4 smart lights will shine, 2 thermostats can regulate, 1 smart fan spins up, 2 blinds should cover, and sensors gauge for motion/temperature/light in rooms.
    - Dataset: Thirty days of synthetic sensor data were generated that included variations in occupancy as well as weather plus user choices for comfort.Users considered were five simulated users showing different lifestyles. These users included someone up early, a night worker, an energy-conscious person, someone prioritizing comfort, and a neutral user.
    - Evaluation Period: 500 recommendations and decision cycles each for every profile.

B. Quantitative Results

Accuracy of Recommendations

- Rule-based systems were accepted at ~65% since they did not personalize enough.
- Pure DQN raised accuracy to about 78%. However, pure DQN is adapted by way of reinforcement learning, often becoming misaligned to unique user choices.
- DQN + Human Feedback reached ~88, 92% accuracy after retraining cycles, also this demonstrated superior personalization

Latency of Recommendations

- Due to the use of static logic, rule-based systems had about the lowest latency (<0.5 sec).
- DQN's inference time was ~1.2 sec. This was with the standalone model.
- DQN incorporating Human Feedback averaged ~1.8 sec because UI confirmation was additional, but stayed under acceptable thresholds (<2 sec).

Trust Score Improvement

- Rule-based systems scored 3.2/5 on trust since users felt constrained by rigid automation.
- DQN alone scored 3.7/5 as it showed adaptiveness but sometimes made errors.

- DQN + Human Feedback achieved 4.5/5 as users felt in control, leading to higher system trust and adoption potential.

Energy Efficiency

- Rule-based automation reduced energy consumption by ~10% compared to manual control.
- DQN achieved ~15% savings through optimized actions.
- DQN + Human Feedback further improved energy efficiency to ~20% by aligning recommendations with real user habits (e.g., avoiding false activations, optimizing thermostat schedules).

VII. CONCLUSION

AI and SIoT have been utilized to analyse an essential application in the Industrial Revolution for securing against cyberattacks, phishing, illicit access, and malware targeting computer network systems. The use of SIoT is helpful for detecting cyberbullying text in multilingual data on SM and home appliances. Identifying these challenges is difficult, especially when controlling SM attacks in various languages and safeguarding users from toxic comments and affects the model performance such as offensive language and verbal assaults. A major issue is maintaining relationships among IoT objects, which requires careful attention to maintain and establish trustworthy connections over time. Therefore, a trust framework in SIoT consisting of aspects of social relationships, object-object interactions, credible recommendations can be built. Optimization techniques are employed to analyse challenges in home applications. AI-based ML methods help identify social network issues. In the future, hybrid AI techniques can be applied to SM to solve the problems analysed in existing works.

REFERENCES

[1] C.-G. Xiang and Z. Yu, "Human-machine hybrid augmented intelligence: Human-machine relationship, collaboration and mutual enhancement," in Proc. China Automation Congress (CAC), 2023.

[2] A. Ali-Eldin, "A hybrid trust computing approach for IoT using social similarity and machine learning," PLOS One, Jul. 2022, doi: 10.1371/journal.pone.0265658.

[3] T. A. Butt, "Edge intelligence-based social Internet of Things for smart cities," in Proc. Int. Conf. Information Technology (ICIT), 2022, doi: 10.1145/3582197.358222.

[4] S. Sagar, A. Mahmood, K. Wang, Q. Z. Sheng, and W. E. Zhang, "Trust-SIoT: Towards trustworthy object classification in the social Internet of Things," IEEE Trans. Netw. Serv. Manag., Jun. 2023, doi: 10.1109/TNSM.2023.3247831.

[5] M. Hosseinzadeh, V. Mohammadi, J. Lansky, and V. Nulicek, "Advancing the social Internet of Things (SIoT): Challenges, innovations, and future perspectives," Mathematics and Computer Science, vol. 12, no. 5, pp. 1–15, 2024, doi: 10.3390/math12050715.

[6] D. Geissler and P. Lukowicz, "Leveraging hybrid intelligence towards sustainable and energy-efficient machine learning," arXiv preprint arXiv:2407.10580, Jul. 2024.

[7] M. Cukurova, "The interplay of learning, analytics, and artificial intelligence in education: A vision for hybrid intelligence," Br. J. Educ. Technol., vol. 55, no. 8, pp. 1432–1448, Aug. 2024, doi: 10.1111/bjet.13514.

[8] K. Krinkin, Y. Shichkina, and A. Ignatyev, "Co-evolutionary hybrid intelligence," in Proc. 5th Sci. School Dyn. Complex Netw. Appl. (DCNA), Kaliningrad, Russia, 2021, doi: 10.1109/DCNA53427.2021.9587002.

[9] S. Khan, F. Amin, and M. Khan, "Modeling of trust in social relationships for secure communication in social Internet of Things," in Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS), 2023.

[10] S. A. A. Bokhari and S. Myeong, "The influence of artificial intelligence on e-governance and cybersecurity in smart cities: A stakeholder's perspective," IEEE Access, vol. 11, pp. 90345–90358, Jul. 2023, doi: 10.1109/ACCESS.2023.3293480.

[11] N. Imran, N. Iqbal, and D. H. Kim, "IoT task management mechanism based on predictive optimization for efficient energy consumption in smart residential buildings," Energy Buildings, vol. 253, p. 111762, 2021, doi: 10.1016/j.enbuild.2021.111762.

[12] S. Fatima, N. Ali, I. Tariq, and N. A. Aslam, "Home security and automation based on Internet of Things: A comprehensive review," IOP Conf. Ser.: Mater. Sci. Eng., vol. 899, no. 1, p. 012011, Jul. 2020, doi: 10.1088/1757-899X/899/1/012011.

[13] P. Rajesh, F. H. Shajin, and G. Kannayeram, "A novel intelligent technique for energy management in smart home using Internet of Things," Appl. Soft Comput., vol. 125, Oct. 2022, Art. no. 109442, doi: 10.1016/j.asoc.2022.109442.

[14] L. Fang and B. He, "A deep learning framework using multi-feature fusion recurrent neural networks for energy consumption forecasting," Appl. Energy, vol. 351, Oct. 2023, Art. no. 121563, doi: 10.1016/j.apenergy.2023.121563.