International Journal of Computer Techniques–IJCT Volume 13 Issue 2, March-April - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

RESEARCH ARTICLE OPEN ACCESS

# A Proactive Défense Mechanism for IoT using AI Agents

Aarti Singh*

*(Asstt. Prof. Computer Science, G.N.G. College, Yamuna Nagar

Email: aartisinghgng@gmail.com)

----------**********----------

## Abstract:

This work introduces an autonomous and secure communication framework for IoT environments driven by AI agents. While IoT is grabbing strong roots in our lives with more and more smart devices being used around us, the security of data collected and the devices as well remains a critical concern. Without robust security measures, these devices can be compromised and are vulnerable for DDOS attacks without the owner's knowledge. While, AI agents have already proved their potential in web-based applications but the potential of these autonomous entities remains untapped in an IoT based environment. especially, for providing security in resource constrained devices.

*Keywords* — **IoT, IoE, Software Agents, intelligent Agents, IoT Security, DDOS Attack.**

----------**********----------

## I. INTRODUCTION

INTERNET OF THINGS (IOT) IS INTERCONNECTION OF PHYSICAL OBJECTS EMBEDDED WITH ELECTRONIC CHIP, SENSORS & ACTUATORS WHICH MAKE THEM CAPABLE OF SENSING DATA FROM THEIR ENVIRONMENT AND COMMUNICATE WITH OTHER PHYSICAL OBJECTS OR HUMAN USERS. IOT MAKES IT POSSIBLE FOR ANYTHING OR EVERYTHING TO BE CONNECTED ON INTERNET AND COMMUNICATE WITH OTHER THINGS WITHOUT HUMAN INTERVENTION. IOT HAS REVOLUTIONIZED THE WAY WE LIVE AND HAS OPENED DOORS TO UNLIMITED OPPORTUNITIES FOR APPLICATION AND SERVICES LEADING TO BETTERMENT OF HUMAN LIVES. SMART HOMES, SMART CITIES, HEALTHCARE MONITORING, CATTLE MONITORING ETC. ARE SOME APPLICATION AREAS OF IOT. FIGURE 1 ILLUSTRATES INTERCONNECTION OF DEVICES PARTICIPATING IN IOT.

Figure 1: Interconnection of devices in IoT (image generated using Chatgpt/DALL-E)

As is clear from figure 1 that any or rather almost all devices participate in IoT and thus such an interconnected system is now being termed as Internet of Everything (IoE). Devices in IoE sense and record information including personal information from the surroundings and communicate it to the controlling device such as mobile, laptop etc. through private and public networks as well. Current generation

personalized web and IoE jointly manage the fast lives of users offering convenience and flexibility in the form of reminders, creating to-do lists, learn and manage user preferences of heating, cooling etc. At the same time these small devices collect personal data also. The devices and the collected data are highly vulnerable to attacks over the network and thus are of utmost concern for research fraternity. For instance, in 2016 DDoS attack on websites including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times was performed through consumer devices working in IoT [5]. Many efforts are being made in this direction, however since devices in IoT are physically small, have constrained resources and limited computational/processing abilities which makes them unsuitable for implementation of existing security mechanisms. This work aims to propose use of intelligent agents in IoE devices and to implement security mechanisms through these agents. Kumar and Patel [1] emphasized that along with the accelerating use of IoT enabled devices in our daily lives, comes acceleration in security and privacy challenges. Further, authors [6,15] have suggested deployment of artificially intelligent (AI) agents in wide array of applications like intelligent manufacturing, traffic and transportation system, communication and cloud based services etc. In the current era of AI, it is clear that achieving a truly secure IoT ecosystem requires more than passive defense; it demands a **proactive, autonomous mechanism** that only **intelligent software agents** can provide. While traditional security struggles with the scale and diversity of smart devices, software agents offer the agility to detect and neutralize threats like **DDoS attacks** in real-time. By porting the proven success of agent technology from web applications to the **resource-constrained** world of IoT, we can build a resilient framework that protects both the data and the devices themselves without human intervention.

This paper is structured as follows: section 2 provides brief overview of software agents. Section 3 presents review of literature. Proposed framework is presented in section 4 followed by conclusion and future scope in Section 5.

## 2. Software Agents: Overview

Software agents find their roots in Distributed Artificial Intelligence, which came in existence in 1970s. Term agent was coined by Carl Hewitt in 1973[14] when he proposed an actor system which could act on behalf of its user. Since then, agents have widely been explored and found applicability in many web-based applications. Agents are possessed with many appealing features which make them promising in diverse disciplines, following are some features of software agents:

- **Autonomous:** can work on their own without human intervention
- **Adaptive:** learn from the choices of their user and adapt according to their interest
- **Reactive:** react to input sensed from their environment, in order to achieve user's goal
- **Proactive:** not only react to input always, they may initiate actions for user's benefit
- **Mobility:** can move from one node to another in the network along with their data and state
- **Persistence:**can work continuously towards their designated goals
- **Social-ability:** have ability to interact with other agents in the network
- **Cooperativeness:**can cooperate and coordinate with other agents for the benefit of their user
- **Goal-oriented:** their actions are directed to achieve their defined goals

Figure 2 given below illustrates features of software agent.


Figure 2: Features of Software Agents (image generated using Chatgpt/DALL-E) for illustrative purpose

Software agents work together in the form of multi-agent systems where multiple agents dedicated to different tasks work collaboratively in order to provide complex services to their users. Software agents have already proved their potential in the field of information retrieval & processing, wireless sensor networks, cloud-based applications etc. thus their potential can be utilized in IoT also. This is the motivation behind proposed work.
Next section provides review of literature in the relevant domain.

## 3. Literature Review

This section explores relevant literature to highlight gaps existing in IoT security and scope of applicability of software agents in this domain. Nguyen et. al [2] highlighted that IoT devices are prone to DDOS attack and replay attacks due to lack of protection methods. IoT devices must include security provisions like confidentiality, integrity, authentication, authorization and freshness to avoid attacks. Authors also emphasized that any security solution must consider constrained resources of devices, ensure availability of network devices even in DDoS attacks, must provide resilience to attacks i.e. attack must not propagate in the network even if one node gets compromised along with privacy protection of the recorded information and scalability of the solution. Sahukat et. al [3] also raised many security threats like securing these gadgets, information and correspondence from unapproved sources. Authors emphasized that new protocols must be developed to address security issues in IoT. As these systems work in highly dynamic environments thus, they must have ability to evolve and adapt. Miorandi et. al [4] stated that IOT builds on three pillars, related to the ability of smart objects i.e. to be identifiable, to communicate and to interact in a network or with user. Developing technologies for enabling such a vision is the main challenge. In [5] authors stated that safety of commercial IoT devices depends on the technologies, protocols and security mechanisms implemented by every individual manufacturer, therefore all IoT devices are vulnerable to certain types of attacks. Thus, there is urgent need of developing general security policies and standards for IoT products.

From the literature review it was observed that research community is emphasizing on need of new protocols for IoT which can meet security requirements in available resources. An analytical look at the available literature [6, 7,10, 11] clearly highlights the viability of introducing AI agents in IoT and thus the motivation for this work.
Singh et. al in [8] proposed a Contract Net Trust Establishment Protocol (CNTEP) which is in fact an extended version of Contract Net Protocol (CNP) [16,17]. It provided mechanism to ensure truthfulness of agents in open, dynamic and heterogenous environments such as IoT. This improved protocol includes trust and reputation parameters to provide secure communication amongst agents working in a dynamic multiagent system which makes it suitable for IoT based applications since attacks in IOT devices can be avoided only by ensuring authentication of participating entities and confidentiality of exchanged messages. This protocol addresses both these aspects. Researchers [5, 9] have highlighted that IoT devices are prone to DDOS attacks and most of DDoS attacks in past are performed by compromising innocent looking home appliances like TV, fridge, microwave etc. Thus, it is very important to protect these devices from malicious access. Singh & Juneja [9] have proposed an agent based system to prevent UDP flood attack in DDoS attack. Iglesia et. al in [12] presented an intelligent mechanism with embedded agents in wireless devices in IoT. Their mechanism used MQTT protocol for communication with semi-closed multi agent system architecture with four layers in architecture. While, the mechanism provided stability, trust, openness and flexibility in communication among devices, however this work further required to analyse alternatives in the security layer to include new paradigms of security and trust for improving the robustness of the system. Nakagawa & Shimojo in [13] presented an IoT agent platform mechanism to separate IOT functions from physical devices and to run IOT functions in isolated cloud environment. In this mechanism every device has a virtual clone in cloud environment which provides all desired IoT functions. However, methods for accessing and updating virtual clones for all participating devices is left as part of future

work. Further, security of the virtual clones so that private information is prevented from unauthorized access is still left unaddressed.
From above review of literature, it is apparent that IoT needs amalgamation of some other technology to provide better security solutions. AI software agents are promising candidates for this purpose. The upcoming section presents an idea and a framework to address the issues highlighted above.

## 4. Proposed Work

This work proposes an *Intelligent Agent based Secure Communication framework for IoT/IoE henceforth termed as (IASCF-IOT)*. It comprises of Home Master Agent(HMA),Home agents ($HA_1$, $HA_2$,---$HA_n$) and Personal Manager Agent (PMA). At present, the devices participating in an IoT network are equipped with sensors to communicate with the outer world. The devices may communicate through any kind of network be it public or private. Home appliances recording sensitive personal data are either not provided with any mechanism for security of device and data or mechanism are not robust due to compact nature of devices and smaller processing abilities. Authors in [2] highlighted that in *existing internet and wireless sensor network communication protocols security mechanisms are poorly defined for communication of devices existing in same network and no provision to protect communication with external entities or on external network*. Thus, there is a severe security loophole in sensor network equipped devices which make them prone to DDoS attacks. DDoS attacks using home appliances and other IoT devices have already taken place and their severity can't be ignored. Presently every IoT device in a home works independently and reports its data to user through its independent application interface. In the absence of strong security mechanism, any outside device can compromise home devices and can make them act as zombies for any attack. The proposed framework embeds an intelligent agent called as Home agent (HA) inside every IoT device. Contract Net Trust Establishment Protocol (CNTEP) [8] is bring into force for establishing the authenticity of HAs in the home network and once authenticated agent are assigned an id number with timestamp of id generation. Since devices and hence agents in home network may join at different time (i.e. all agents may not get registered at the same time), the first device to get registered with PMA will be designated as HMA and is responsible for coordinating communication. All home agents communicate with HMA and are restricted to communicate with any external entity not having internal network id assigned by HMA. This prevents devices from getting compromised for DDoS attacks. Within the home premises, each appliance performs its job and report to HMA which in turn communicate with PMA installed in mobile device of user. In this system, HMA is a mobile agent capable of moving across network along with its state and data. Interaction between HMA and PMA could be seen on public network. In such a case HMA rather than sending message in the form of traditional insecure packets, transits itself from home network to user's device in encapsulated form, communicates required details to PMA and comes back, thus ensuring secure communication even in public networks.
Figure 3 illustrates high level view of proposed framework.

Detail of various agents in the proposed framework is as follows:

- ***Home_Master_Agent (HMA)***: This agent is responsible for registration of all devices in home network using CNTEP[8]. HMA checks certified reputation of respective home agent by checking authentication certificate provided by manufacturing company. Once authenticity of HA is proved, it assigns homenetworkid (HN_id) to that agent and records the same in Home_network_table (HNT) for future reference, this table is accessible to all agents of this multiagent system. HMA is mobile agent capable of travelling across public network.
- ***Home_Agent (HA)***: Whenever a new device is installed in home network, it gets itself registered in the same through HMA and gets its id. Once registered, device performs its

intended job and sends data to user through HMA. Every such communication is performed through message comprising of <HN_id, data> pair. Home agents may communicate with each other if required using the same message pair. In case any outsider device tries to communicate with any device in home network, it is not be able to provide its HN_id and communication is blocked, thus preventing the device to be compromised. Since there are many participating devices in home network IoT system, first device to be registered with PMA acts as HMA.

- ***Personal Manager Agent (PMA)***: This agent acts as interface between user and home network. It communicates with all devices in home network through HMA. When the user is in home network, communication takes place between HMA and PMA through message pair, but when PMA is somewhere in public network, then instead of sending message in public network, HMA transmits itself in the network and exchanges message with PMA, thereby providing data security.

Working of the proposed mechanism is depicted in flowchart given in Figure 4.

Working of various agents is given in figure 5(a)-5(d) Figure 5(a) and 5 (b) provides algorithm of HMA for registration of HA and for performing communication.

## 5. Conclusion and Future Scope

This work proposed an intelligent agent-based proactive defense framework for secure communication in IoT. Agent technology is well established and widely deployed in internet-based applications, thus it can surely be deployed in IoT scenario. Further, agents may be developed on Java based open-source platform such as JADE which make them suitable for constrained device. This work uniquely contributes by ensuring agent communication through contract net trust establishment protocol which ensures trustworthy and reliable communication among agents in a multi agent system. The security of HMA while migrating on a public network is worth addressing in future.

## REFERENCES

[1] J.S.Kumar& D.R. Patel , *A Survey on Internet of Things: Security and Privacy Issues*. Published in International Journal of Computer Applications, Vol. 90, No. 11, March 2014, pp.20-26, ISSN: 0975 – 8887.

[2] K.T. Nguyen, M.Laurent, N.Oualha, *Survey on Secure Communication Protocols for the Internet of Things*. Published in Elsevier Journal of Ad Hoc Networks, Volume 32,2015,Pp 17-31,ISSN 1570-8705.https://doi.org/10.1016/j.adhoc.2015.01.006.

[3] K. Shaukat, T. M.Alam, I. A. Hameed, W.A.Khan, N.Abbas,S.Luo, *A Review on Security Challenges in Internet of Things (IoT)*, Published in Proceedings of the 26th International Conference on Automation & Computing, University of Portsmouth, Portsmouth, UK, 2-4 September 2021.

[4] D.Miorandi, S. Sicari, F.D. Pellegrini, I.Chlamtac, *Internet of things: Vision, Applications and Research Challenges*, Published in Elsevier Journal of Ad Hoc Networks, Vol 10, 2012, pp. 1497-1516.

[5] Y. Yang, L. W.G. Yin, L.Li, H. Zhao, *A Survey on Security and Privacy Issues in Internet of Things*. Published in IEEE Internet of Things Journal, Vol. 4, Issue 5, pp.1250-1258, October 2017.

[6] D. Juneja, A. Singh, R.Singh, S. Mukherjee, *A Thorough Insight into Theoretical and Practical Developments in MultiAgent Systems*. Published in International Journal of Ambient Computing and Intelligence,Volume 8, Issue 1, January-March 2017, pp. 23-49.

[7] A. Singh, D.Juneja, A.K.Sharma, *Agent Development Toolkits*. Published in International Journal of Advancements in Technology, Vol.2, No.1, January 2011, pp.158-164.

[8] A. Singh, D.Juneja, A.K.Sharma, *Introducing Trust Establishment Protocol in Contract Net Protocol*. Published in proceedings of IEEE International Conference on Advances in Computer Engineering (2010), pp. 59-63.

[9] Article on *Common Cyber-Attacks in the IoT* by Globalsign by GMO .Avaliable online at **https://www.globalsign.com/en/blog/common-cyber-attacks-in-the-iot**. Accessed on March 13,2026.

[10] http://www.jade.tilab.com

[11] http://www. fipa.org

[12] H. De La Iglesia, D., Villarrubia González, G., Sales Mendes, A., Jiménez-Bravo, D. M., & L. Barriuso, A. (2019). *Architecture to Embed Software Agents in Resource Constrained Internet of Things Devices*. *Sensors*, *19*(1), Article No. 100. https://doi.org/10.3390/s19010100 .

[13] I. Nakagawa &S. Shimojo (2017, July), *IoT agent platform mechanism with transparent cloud computing framework for improving IoT security*. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2, pp. 684-689. IEEE.

[14] C.Hewitt, P. Bishop & R. Steiger (1973 August). *A Universal Modular Actor Formalism for Artificial Intelligence. Proceedings of the 3rd international joint conference on Artificial intelligence* (pp. 235-245). Morgan KaufmannPublishers Inc.

[15] Franziska Klügl, *Applications of Software Agents*. Journal of Künstliche Intell. 18(2): 5-10 (2004).

[16] Alibhai Z., *What is Contract Net Interaction Protocol?* .IRMS Lab, SFU, Jul. 2003.

[17] Wu J., *Contract Net Protocol for Coordination in Multi-Agent System*. Proc. of 2nd Intnl. Symposium on Intelligent Information Technology Application, pp. 1052-1058, 2008.

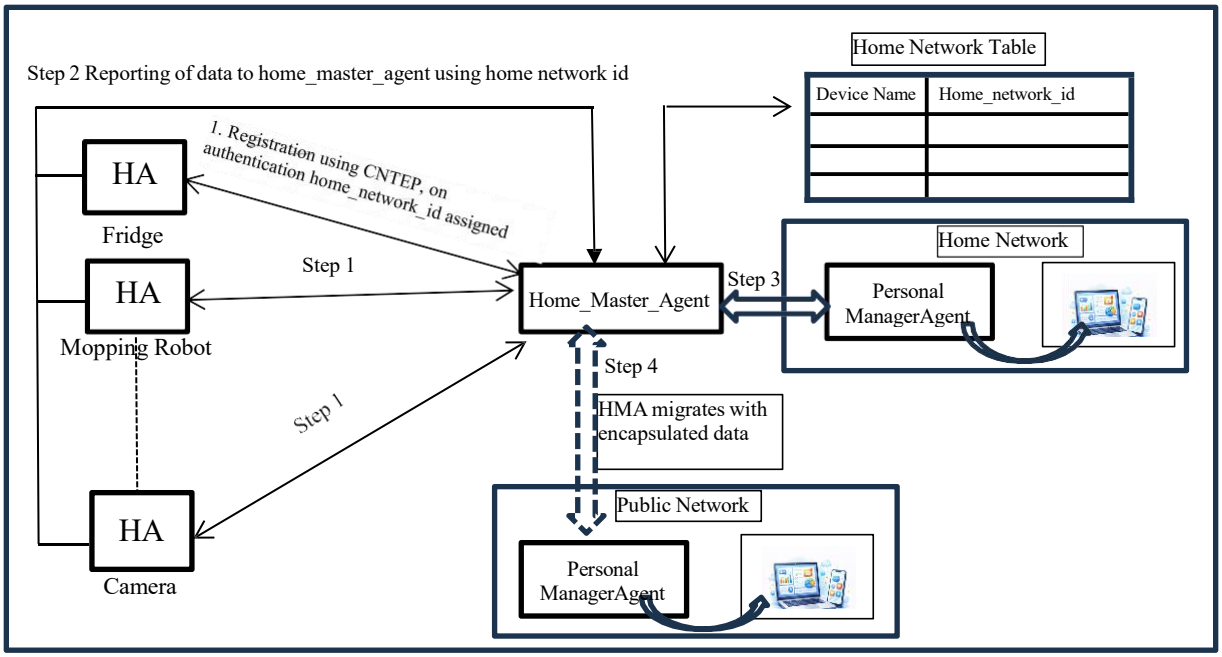


Figure 3: High level view of Intelligent Agent based Secure Communication Framework for IoT (IASCF-IOT)

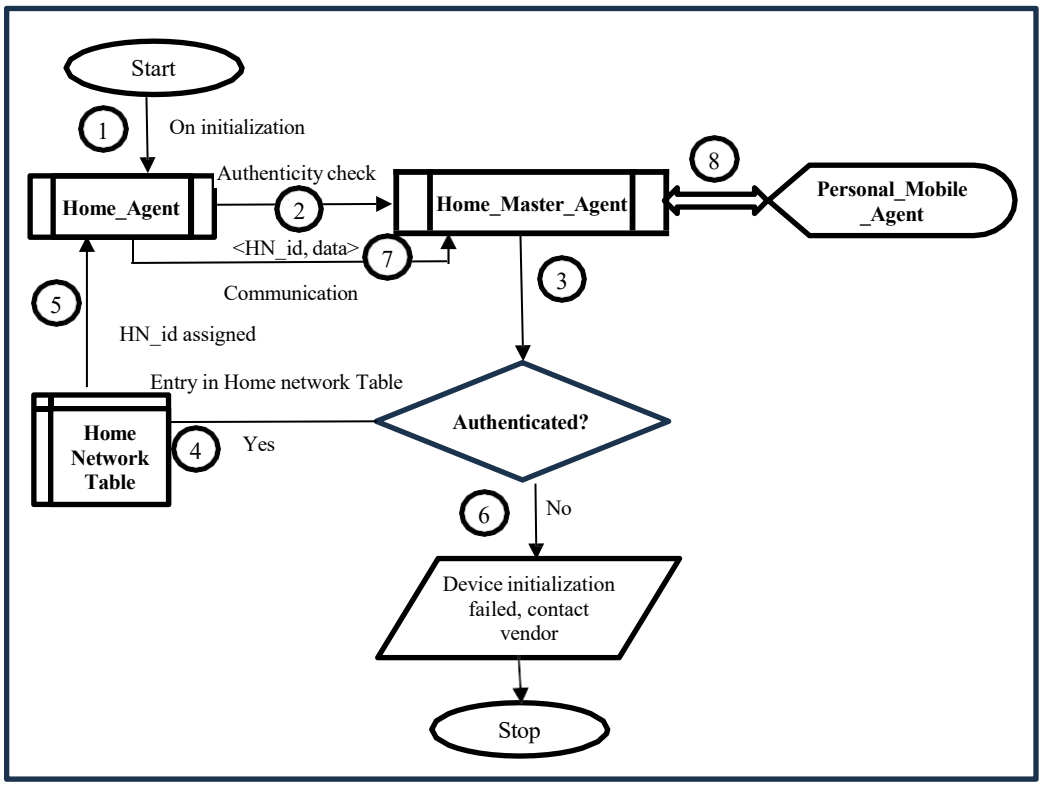


Figure 4: Flow chart of proposed framework

```
Home_master_agent( )
{
input: registration_request from HA_i,authentication_certificate;
output: HA_i registration on authentication,id assignment;
on registration_request(HA_i)
{
receive (authentication_certificate) from HA_i ;
Check certificate validity from source;
If (valid)
{ register HA_i in HNT;
send HN_id to HA_i for further communication;
}
else
{ send HA_i ← message(authentication_failed);
block communication;
}
}
```

Figure 5 (a): Algorithm of HMA for registration of HA

```
Home_master_agent( )
{
input:communication request from HA_i or PMA;
output:performing communication;
{
 if request ← HA_i(data_reporting)
{ accept<HN_id, data> ← HA_i ;
send communication request to PMA;
receive location (PMA);
If (location(PMA)==Home_network)
send PMA ←<HN_id,data>;
else
{
encapsulate (data);
migrate (location(PMA));
}
revert instruction to HA_i ;
}
```

Figure 5(b): Algorithm of HMA for facilitating communication

```
Personal_master_agent( )
{
input: information request from user; information received
from HMA();
Output: take action to fulfil user request;
on request from user
{call HMA();
forward user request to HMA();
 }
on receiving input from HMA()
{send input to user;}
}
```

Figure 5 (c): Algorithm of PMA

```
Home_agent( )
{ input: data sensed ;
Output: registration request to HMA();
communication with HMA();
on initialization
{
send registration_request → HMA();
send authentication_certificate → HMA on request ;
Receive HN_id from HMA;
}
On need_for_communication
{ send<HN_id, data> to HMA;}
On receiving communication_request
{check HN_id of sender from HMT;
 if (invalid HN_id)
{block communication;}
}
```

Figure 5 (d): Algorithm of HA