**INTELLIGENT AGENTS DEFENDING FOR AN IoT WORLD: A REVIEW**

**209074206**

**FAKOREDE OLUMIDE DANIEL**

**TABLE OF CONTENT**

Cover Page i

Table Of Contents ii

List of Figures iv

List of Tables iv

Abstract v

**CHAPTER ONE – 1.0 INTRODUCTION 6**

1.1 Problem Statement 7

1.2 Aim and Objectives 8

1.3 Methodology 11

1.4 Definition of Terms (Dasgupta et al, 2020) v

**CHAPTER TWO – 2.0 LITERATURE REVIEW 12**

2.1 Historical Perspectives 12

2.2 Previous Work 12

2.3 Summary of Previous Research 13

**CHAPTER THREE – 3.0 ARCHITECTURE/CONCEPTUAL MODEL 17**

3.1 Theoretical Framework 17

3.1.1 Reflexive Process 17

3.1.2 Soft State 18

3.1.3 Medium State 18

3.1.4 Hard States 19

3.2 Architecture of the proposed system 20

3.3 Technical Details 22

**CHAPTER FOUR – 4.0 APPLICATIONS 23**

4.1. Home Automation 23

4.2. Smart Cities 23

4.3. Smart Retail 24

4.4. Animal Farming and Smart Agriculture 24

4.5. Smart Grids and Smart Metering 24

4.6. Smart Environment 25

4.7. Security and Emergencies 25

**CHAPTER FIVE – 5.0 CONCLUSIONS 27**

**REFERENCES 28**

**LIST OF FIGURES**

Fig 3.1: Soft State representation of ML techniques 18

Fig 3.2: Medium State representation of ML techniques 19

Fig 3.3: Hard States representation of ML techniques 20

Fig 3.4: Autonomous process 20

Fig 3.5: Intelligent Agent defense cycle transitions 21

**LIST OF TABLES**

Table 2.1: Shared Contexts 14

**ABSTRACT**

The interaction with environment has observed a great change due to the introduction of internet of things ranging from household gadget to sophisticated machine for industries However, the interconnection brings numerous security challenges that are more than traditional cybersecurity measures can handle. The diversity of IoT devices, with their varying computational capabilities and communication protocols, makes them open to diverse cyber threats. Conventional intrusion detection systems struggle to cope with data coming from IoT devices are of various form which are evolving nature of attacks. This review examines the publication that involve the detection of instruction in IoT domain using intelligent agents as a viable solution. Intelligent agents, and their ability to independently learn, adapt, and collaborate, present a hopeful strategy for tackling the distinct challenges in the IoT environment. Various intrusion detection approaches, models as intelligent agents, and identifies key requirements and challenges for deployment in IoT environments

**CHAPTER ONE**

**1.0 INTRODUCTION**

The emergence of the machine-to-machine device (M2M) or IOT is the reason for the paradigm shift of how we interact with devices and systems around us. The interconnection of heterogeneous devices, ranging from household appliances to industrial machinery, has opened up a world of possibilities for automation, efficiency, and convenience (Perera et al., 2014; Xu et al., 2014; Zanella et al., 2014).

However, this interconnectivity also introduces new security challenges that traditional cybersecurity measures may not be equipped to handle effectively. The IoT ecosystem consist of a number of devices with varying computational capabilities, operating systems, and communication protocols. These devices mostly do not have robust security features, which make them vulnerable to attacks and exploits (Stankovic, 2014).

The sheer volume of data coming from IoT devices presents a significant challenge for intrusion detection and prevention systems (IDS/IPS) (Desai et al., 2015; Rivera et al., 2015). Traditional IDS/IPS solutions, which rely on signature-based detection or anomaly-based detection techniques, may not scale well in the IoT environment (Coulter and Pan, 2018). Signature-based detection can only identify known threats, leaving the system vulnerable to zero-day attacks. Anomaly-based detection, these device can generate high number of false positives, leading to increased operational costs and inefficiencies (Sobh, 2006).

Internet of Things (IoT) cuts across various devices, including industrial systems, intelligent sensors, autonomous vehicles, mechanisms and terminals, mechanical systems, etc (Al-Fuqaha et al. 2015, Sharma et al.2020).

On the other hand, it is seen as an object of things or machine to machine that is connected together with less communication efforts, low computation power, and less storage capabilities linked together with embedded electronics such as sensors and actuators. This is the connection of network and software that makes it possible for these devices to exchange, analyze, and collect data (Hussain et al. 2020). our everyday life is related to IoT, this includes smart devices used in households, for instance smart meters, smart adapters, smart bulbs, IP cameras, smoke detectors, smart refrigerators, AC, smart ovens, and temperature sensors, to more sophisticated devices, like accelerometers, heartbeat detectors, IoT in automobiles, radio-frequency identification (RFID) devices, sensors in rooms, and many more (Hussain 2017). Various services and applications that can be linked to the IoT are evolving from personal healthcare to home appliances to critical agricultural infrastructure, and the military (Al-Fuqaha et al. 2015). The challenges many Internets of Things devices face include tools management, the quantity of data and storage used for communication, methods employed to process data, and privacy concerns. Researchers has come up with different journal which cut across various components of this device which includes architecture, communication, applications, protocols, security, and privacy, to name a few

**1.1 PROBLEM STATEMENT**

Intrusion detection and prevention systems are faced with some limitations due to the sophisticating nature of the Internet of Things ecosystem. Data come from IoT devices are vast the present systems available cannot handle it, these solutions are posed with the diversity in the communication of protocols, and varied computational capabilities of the internet of Things also they are faced with security issues which make it in efficient for wide range attacks, such as zero-day attacks, which the present-day signature detection method cannot handle (Coulter, 2018). The limitations of current Intrusion Detection System and Intrusion Prevention System tools in the IoT context have led to a growing interest in the development of intelligent, adaptive, and autonomous intrusion detection agents capable of addressing the unique challenges of this environment (Coulter and Pan, 2018; Zhao and Ge, 2013). These intelligent agents must be able to learn and adapt to new threats, collaborate with other agents in a distributed manner, and take autonomous actions to mitigate or prevent attacks (Igbe et al., 2016; Liu et al., 2012; Sreelaja and Pai, 2014)

**1.2 AIM AND OBJECTIVES**

This review investigates how current intrusion detection approaches fulfill the role of intelligent agents, the requirements for autonomous action against compromised intelligent and distributed IoT nodes, and the vulnerabilities, challenges, and applicable methodologies. The objectives are as follows

1. Review literature on traditional and distributed intrusion detection approaches, and model them as intelligent agents for an IoT perspective.
2. Define and identify various key terms across intrusion detection, AI, and IoT domains,cycle needed for defensive agents, relevant manufacturing and security challenges, and considerations for future development.
3. Investigate available solutions and propose suggested solutions and enhancements to existing intelligent agents defending an IOT world, focusing on refining strategies that integrate recent advancements in machine learning and artificial intelligence

**1.3 METHODOLOGY**

To achieve the stated aim and objectives, this research will employ a combination of theoretical and empirical methods, drawing from the fields of computer science, cybersecurity, artificial intelligence, and multi-agent systems.

1. A comprehensive review of existing literature will be conducted to gain a thorough understanding of the current state of intrusion detection and prevention techniques, focusing on their applicability and limitations in the IoT context. This will involve analyzing research papers, technical reports, and industry publications related to IoT security, multi-agent systems, machine learning, and artificial intelligence.
2. A discussion of the characteristics and types of intelligent agents, as well as their applications in IDS.
3. The review will also include a discussion of the challenges and limitations of using intelligent agents in IoT security.

**1.4 Definition of Terms** (Dasgupta et al, 2020)

1. **Internet of Things (IoT):** a network machine interconnected together containing sensors, software, and other technologies for data collection and exchange between other devices and systems over the Internet.
2. **Intrusion Detection System (IDS):** a security system that is used to monitor interconnected systems activities for illegal acts or policy violations and produces reports to a management station.
3. **Intrusion Prevention System (IPS):** A security system that is used for monitoring network or system activities for malicious activities, automatically takes action to block or prevent those activities and generate reports send the reports to a management station.
4. **Signature-based Detection:** A method used by Intrusion Detection System and Intrusion Prevention System systems to identify known threats by comparing network traffic or system activity patterns against a database of predefined signatures or patterns associated with known attacks.
5. **Anomaly-based Detection:** A method used by IDS/IPS systems to identify abnormal or suspicious activities that deviate from established baselines or behavioral norms.
6. **Zero-day Attack:** A cyber-attack that exploits a vulnerability in a system or software that is unknown to the vendor or security community, thus leaving no time to develop patches or defenses before the attack occurs.
7. **Intelligent Agents:** Software entities that possess the ability to learn, adapt, and act autonomously to accomplish specific tasks or goals in complex environments.
8. **Multi-Agent Systems (MAS):** A device that has multiple interactions of intelligent agents that can collaborate, communicate, and coordinate to solve problems or achieve goals beyond the capabilities of individual agents.
9. **Machine Learning (ML):** the area of artificial intelligence that helps systems to self-learn and improve from experience without being explicitly programmed.
10. **Deep Learning:** the part of machine learning that is used for artificial neural networks with many layers used in processing large data inputs and extract high-level features.
11. **Autonomous Agents:** Intelligent agents capable of operating and making decisions independently without human intervention.
12. **Smart Devices:** devices that are connected with sensors, actuators, and connectivity that enable them to get and exchange data, as well as interact with their environment or other devices.
13. **Smart Home:** house that have smart devices and home automation systems that allow homeowners to remotely control and automate household functions such as lighting, heating, ventilation, air conditioning, appliances, and security.
14. **Smart City:** A city that uses information and communication technologies (ICT) to enhance the quality of urban services, reduce resource consumption and overall costs, and improve the citizens' quality of life.
15. **Ensemble method:** Machine learning technique that combine multiple classifier algorithm to improve the performance of the model over individual models.
16. **Firewall:** A network security device or software that is used to monitor or control network traffic coming out or going in based on predetermined security rules.
17. **Access Control:** A security measure that regulates who or what can view or use resources in a computing environment.
18. **Cloud Computing:** The use of computing services such as servers, storage, databases, networking, software, and analytics over the internet to offer innovation, flexible resources, and economies of scale.
19. **Machine Perception:** The ability of a machine or intelligent agent to interpret and understand sensory inputs, such as images, sounds, and text, similar to human perception.
20. **Artificial Neural Networks (ANN):** A computational model that is build based on the function of biological neural networks in the human brain, used to approximate functions that can depend on a large number of inputs and are generally unknown.

**CHAPTER TWO**

**2.0 LITERATURE REVIEW**

**2.1 Historical Perspectives**

Different approaches are present to keep the network and its related devices from attack. firewalls are hardware or software tools that allow or refuse communication inside the boundaries of a network or device. An intrusion detection system (IDS) monitors the network traffic to determine intrusion attempts; successful attempts may be documented or trigger an alarm. Intruder prevention systems improve detection capabilities by actively stopping connections that violate established restrictions, such as dropping communications. Three detection methods include signature-based, anomaly-based, and specification-based (Sobh, 2006). The models' environmental placement might be based on the host or the network. Network-based or NIDS aims to monitor how network traffic is transmitted, whereas host-based HIDS monitors a single host's activities, system calls, and logs (Sobh, 2006). Artificial intelligence is a discipline that has made several contributions in revealing the concepts, ideas, or practical methods utilized in intelligent systems or applications. To understand this we need to consider the research made by Russell et al. (2003) where they published Artificial Intelligence as a Modern Approach, that is valuable for academic teaching or providing a cohesive reference to the area of Artificial Intelligence (AI). The ideal rational agent has not been produced; if it exists, we would not be required to construct agents but would reassign their functionality. Our IoT ecosystem will require different variety of autonomous agents (Desai et al., 2015; Rivera et al., 2015). the physical environment is detected and weighed through nodes that enhance the provision of services or information to smart applications. Perception, Network, and Application layers are present in the architecture (Gou et al., 2013; Zhao and Ge,2013). Another architecture modeling allows a Perception, Network, Middleware, Application, and Business layer (Khan et al., 2012).

A new problem is the growth of the Internet of Things, or everything (IoT), which needs a communication path to connect the physical and cyber worlds. The integration of linked systems, objects, and devices, both homogeneous and heterogeneous, provides access to a wealth of services, information, and applications (Perera et al., 2014; Xu et al., 2014; Zanella et al., 2014).

**2.2 Previous Work**

Several attempts have been made to incorporate intelligence into defense models for the detection of abnormal behavior; obviously, several reviews have been conducted in this area. Alsmadi and Xu (2015) examine the security controls of software-defined networks, including firewalls, access control, IDS/IPS, policy, monitoring, and auditing as cloud intrusion detection techniques proposed by Modi et al. (2013), and alarm management in by Patel et al. (2013), IDS/IPS technologies, approaches and methodologies in Liao et al. (2013) work and the use of Ensemble techniques in Folino and Sabatino (2016) review.

Wu and Banzhaf (2010) review computational intelligence and its accompanying algorithms. From their results, it can be concluded that insider threats or challenges of adaptation of the systems used for detection and the scalability of nodes, and data volumes linked with it are confined to concerns of the environment. It has also been discovered that the bulk of the literature studied focused on data optimization and analysis, that represents the sensing element of these systems. Real-world intruder systems have similar challenges with their functionality (Keung et al., 2012; Mohapatra et al., 2016). However, if we draw any conclusions from the examined literature, we can identify a common strategy to intelligent intrusion detection. Deployment cycles employ four essential steps to detect aberrant activity in the system via monitoring: information is taken from important characteristics, and aggregation techniques are performed to better define sites of interest and enhance anomaly detection. A lot of information may be gathered by handling the surrounding data used to test and train IDS agents, however, the design of these systems has inherent limitations in an IoT environment, including autonomous action and security analysis. There are benefits to using an IDS system to monitor perimeter edge traffic, but it will still operate in traditional mode, without the necessary intelligence and autonomy (Rivera et al., 2015).

**2.3 Summary of Previous Research**

The combination of Intruder Detection, Artificial Intelligence, and the Internet of Things domains has common attributes. In bringing together further development of smart security in an IoT area, a common area of IOT is summarized in table below

Table 2.1: *Shared contexts: Common items that overlap between the Artificial Intelligence, Intrusion Detection, and the Internet of Things domains (Coulter and Pan, 2018).*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Intelligent agent (Russell et al., 2003)** | **IDS (Lugo-Cordero and Guha, 2013; Sobh, 2006)** | **IoT (Desai et al., 2015; Rivera et al., 2015; Zanella et al., 2014)** | **Context definition** |
| Agent | The Physical or software that can interact logically with its environment | IDS device or software installation of varying operational ability and autonomy | IoT device with capabilities of intelligence and reasoning | An instance of an IDS that contains a given level of intelligence |
| Sensor | This means for the input of the agent’s environment. Imagery, Audible, Environments, etc. | An IDS device Network Interface Card (NIC) or simple IP device (fixed or wireless) | Small wireless IP device of limited processing, energy; either IP or combined with environmental sensing abilities | Small form factor device that transmits via IP, fixed or wireless communications, Combined with IDS and possibility for environment sensory input |
| Effector | Provides the ability to interact with environment | A decision that results in alteration of network characteristics or traffic | Physical or software that grants ability to interact | Element for an agent to interact with the environment |
| Percept (sequence) | Perceived history | Perceived history | Perceived history | The observed history of an agent |
| Autonomy | A means to act independently | A means to act independently | A means to act independently | Ability to act independently |
| State | Understanding of environmental condition | Operational mode, condition of its being, or state analysis of connection | Operational mode or condition of its being, | Conditional being and environment conditional memory |
| Goal | The objective of the ideal state | Achievement of the given action | Achievement of the given action | Task, Ideal state, Objective, etc. to achieve |
| Utility | The performance measure for achieving the goal | Value associated with goal, or purposefulness | Value associated with goal, or purposefulness | Achievement measure: |
| Critic | External party, determine success and means providing feedback | External expert or node (i.e., specification based) | Node or control head | External expert or master node/device |
| Node | Data reference within the search tree | Reference to the device or sensor | Reference to the device or sensor | Reference to the device or sensor |
| IDS | N/A | Intruder Detection System | Intruder Detection System | Intruder Detection System |
| Multi-agent | Multiple versions of Agent may be independent of each other | Multiple versions of Agent may be independent of each other | Multiple versions of Agent may be independent of each other | Multiple versions of Agent may be independent of each other |

**CHAPTER THREE**

**3.0 ARCHITECTURE/CONCEPTUAL MODEL**

**3.1 Theoretical Framework**

Present-day detection systems classified knowledge as either misuse or anomaly detection, it is both reflex and model-based intelligence. Security experts have already defined environmental conditions as conditional rules for agents as a tool for monitoring. these deployments fit a reflexive model. Machine Learning combines memory functionality that allows agents to recall an instance or occurrence and an associated class, thereby keeping an internal state aligned with model agents. Typically, single-instance deployments that sniff, log, or alert in a real-time or historical environment based on threat cost has been existing defining the mechanisms which is classified according to growing intelligence ability or reflexive and model processes in soft, medium, and hard states.

**3.1.1 Reflexive Process**

Simple reflexive agents display Snort and Bro deployments, with predetermined intelligence or programmed logic, and no knowledge of state variables is retained. Configurable extras, such as the preprocessor, maintain limited knowledge per target instance based on programmed requirements. Considering rule-based detection methods rather than signature libraries. Signature detection is created after an assault has happened; it is necessary to aid in the development of more reactive techniques. A combined effort based on user scenarios and supplied qualities resulted in rule recommendations (Sonchack et al., 2015) via a defined knowledge base. Data processing (cleaning, reduction, standardization, etc.) is combined with k-means clustering for abstraction with data mining techniques (Haque et al., 2012), and Ji et al. (2016) perform numerical and binary processing to further enhance model understanding, aided by Support Vector Machine (SVM), and rule pattern analysis for dynamic construction in reducing rule libraries (Chen et al., 2009). Lin et al. (2012) analyze the datasets required for state information used in rule creation using Simulated Annealing (SA) and SVM for parameter optimization, followed by SA and Decision Tree (DT) for decision rule formulation. The results of these processes enable the design of rules based on expert or machine intelligence.

**3.1.2** **Soft State**

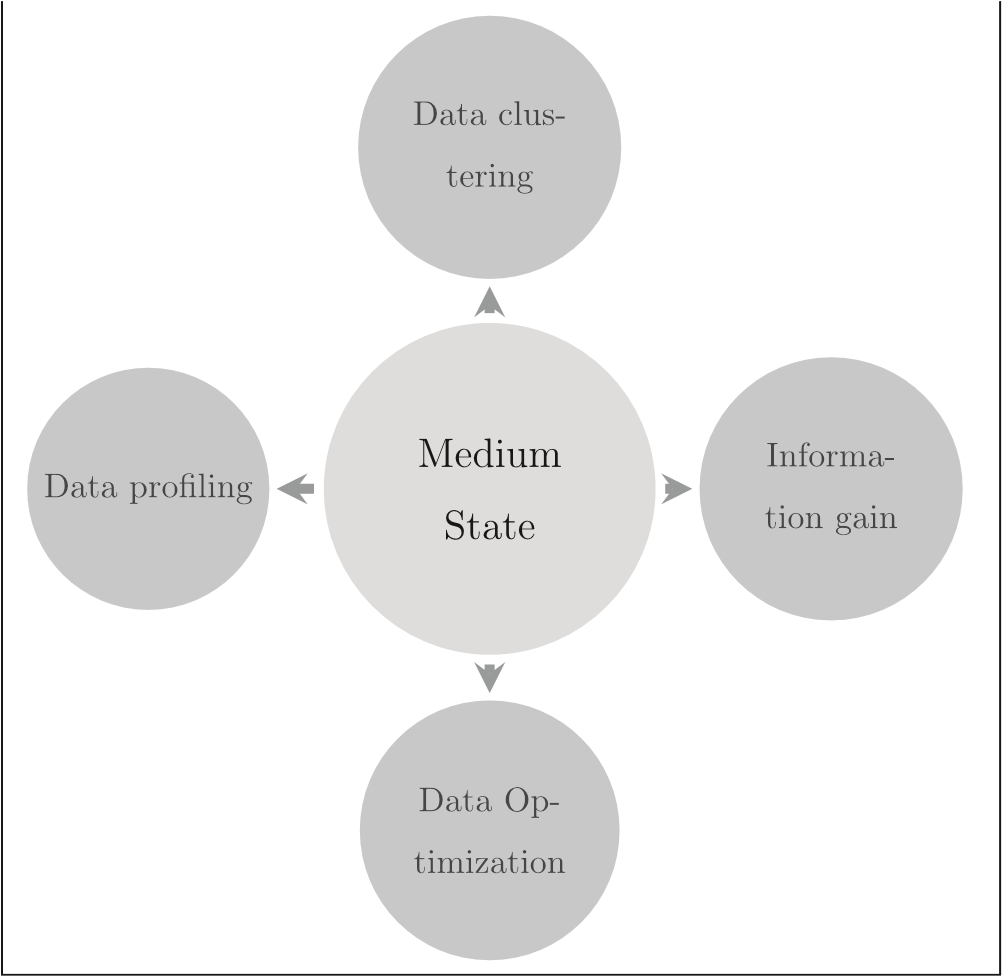
Machine learning is needed to build more proper agents for this to be achieved several states or steps are required the soft states explain the data normalization and feature selection phase of the learning process of the machine

*Fig 3.1:* *Soft State representation of ML techniques: light data analysis, adjustment, and*

*optimization are conducted. (Fang and Liu 2011)*

**3.1.3** **Medium State**

This approach as seen in the images below tries to optimize the dataset to define the state view. The performance of machine learning depends on how the data represents the state space trained with, a good representation leads to better results and feature selections allow noise to be removed from the dataset enabling smooth learning (Armanfardet al., 2016; Bengio et al., 2013). Sangkatsanee et al. (2011) use classification and processing with decision trees to gain feature information, Lin et al. (2015) use clustering and neighbor distance with Known Nearest Neighbor (k-NN), and Tsai and Lin use area triangulation of k-Means clusters to train a (k-NN) classifier.

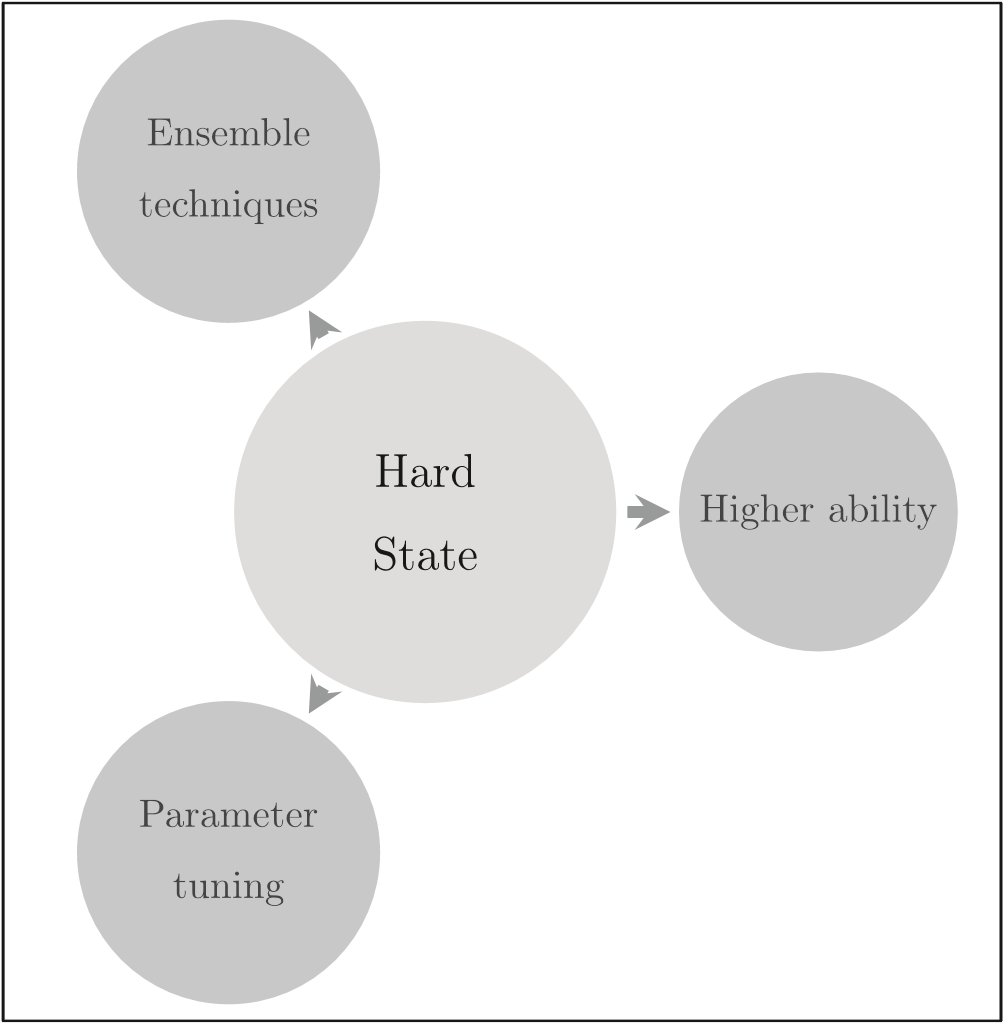


*Fig 3.2: Medium State representation of ML techniques: data optimization is focused on best representing features, elements, or representation of*

*attacks. (Sangkatsanee, et al. 2011)*

**3.1.4 Hard States**

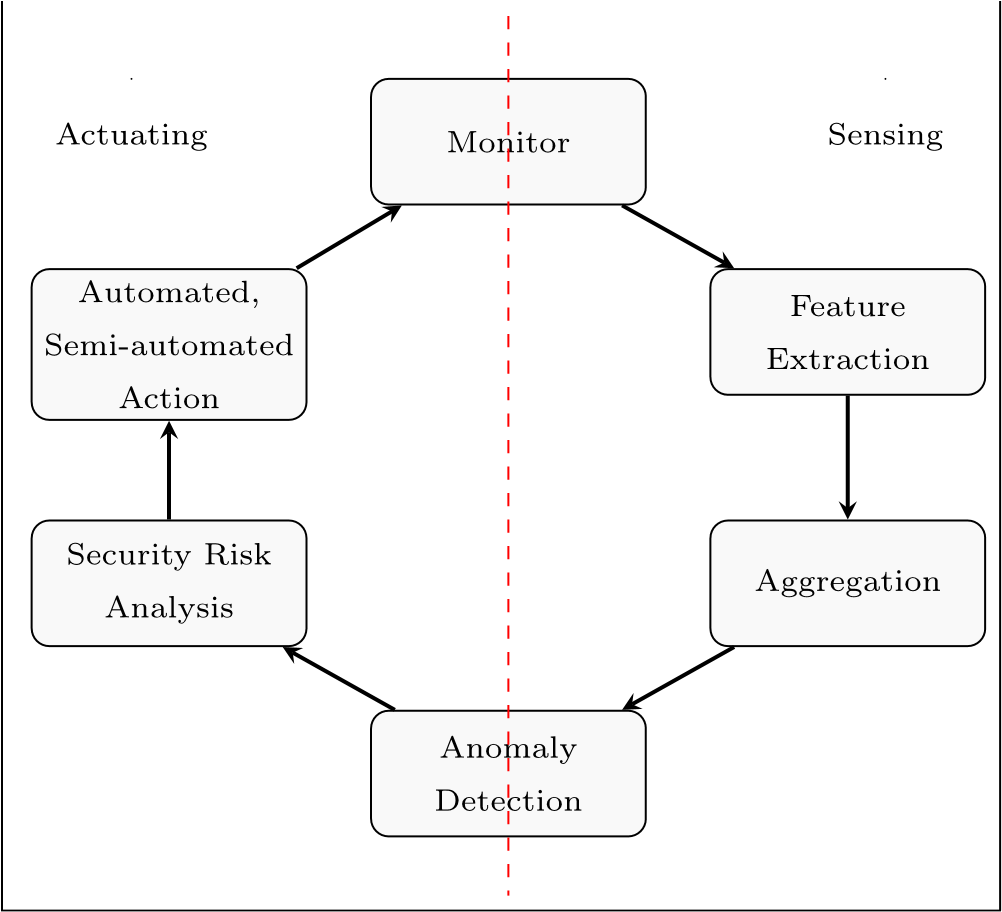
The hard state is used to define how the ensemble method, parameter tuning, and higher-level agent ability are incorporated for the state adjustment. This state can also allow the classification that will determine the nature of intrusion attempts in having as complete percept sequence as possible, the most rational decision may be made (Bengio et al., 2013).



*Fig 3.3: Hard States: Considerable steps are undertaken to improve the data used for sensing by agents. (Bengio et al., 2013)*

**3.2 Autonomous Process Architecture for Intruder Detection**

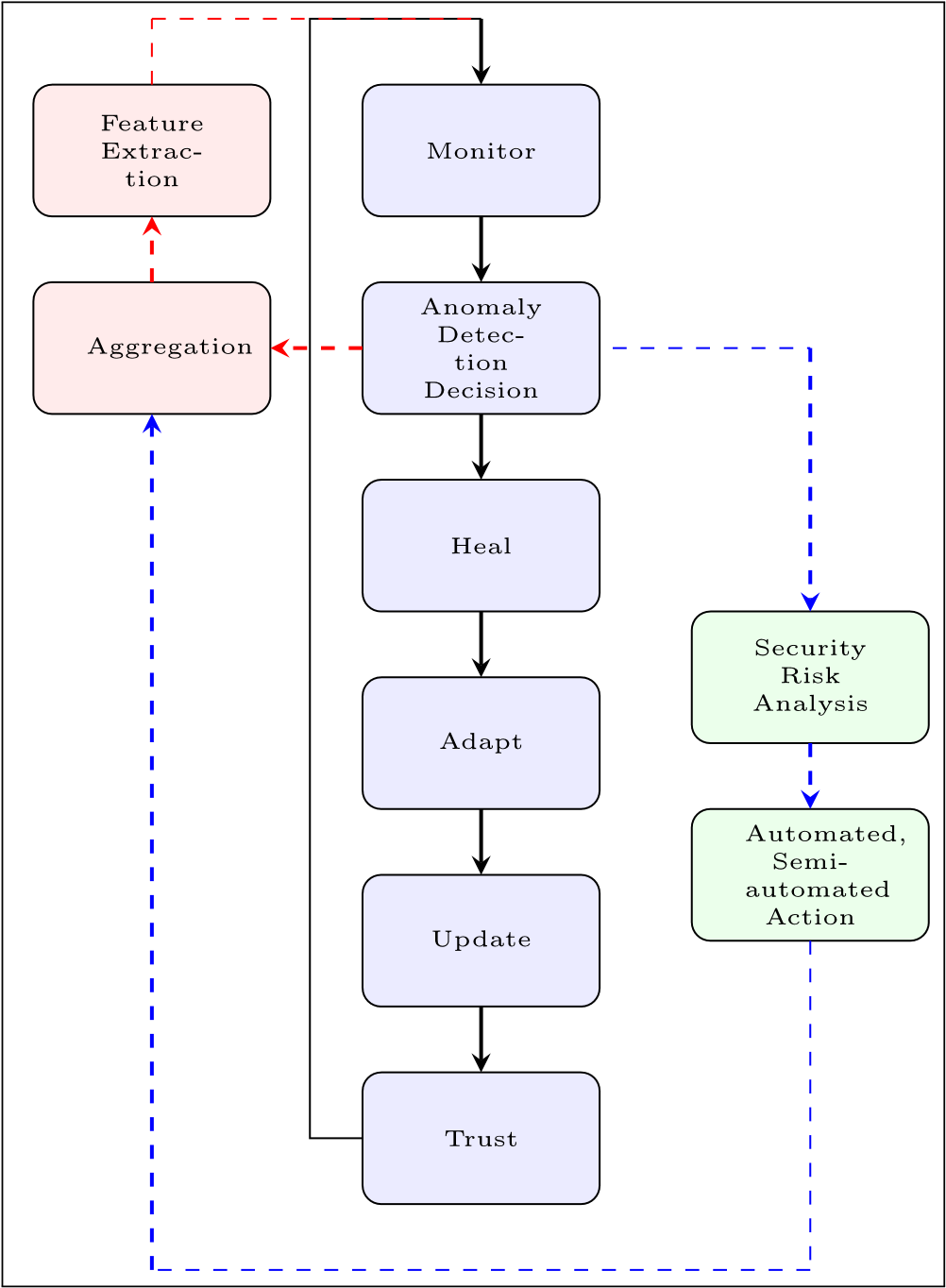
This review examines the use of two-side cycles in approaches to intruder detection system agents in its deployments as seen in the figure 3.4.



*Fig 3.4: Autonomous process: considerable effort has been applied to the Sensing operations in establishing IDS systems. Attacks and threats continually evolve, so too*

*should defensive agents. (Coulter and Pan, 2018).*

It can be observed from the right side of the perforated red line, a general approach, here the feature extraction of information is followed by monitoring of the network the end it is aggregated to make detection decisions, repeatedly. This same circle is found in the full architecture below



*Fig 3.5: Intelligent Agent defense cycle transitions (Coulter and Pan, 2018)*

The left uppermost loop of Fig 3.4, depicted in black and red lines, is shown on the left-hand side of Fig 3.4, where the introduction of autonomous processes based on security policy requirements is completed following the sensing processes. This increasing cycle from sensing is shown by the perforated blue lines in Fig. 3.5, which form the outside right-hand loop. As can be seen in Fig. 3.4, a full loop follows the stages of monitoring and detection, then the blue loop via the red loop and back to monitoring. The inner black-lined loop represents the start of a defense cycle for IoT defensive agents. It contains the entire loop of Fig.3.4 or the red outer top and blue lower left loops of Fig. 3.5; its inclusion ensures the end of the outside loop because it encompasses both. Elements are brought out into new stages for agents to boost collaborative effort and operational efficiency. The new cycle represents the emergence of the desire to have agents operate more autonomously.

**3.3 Technical Details**

An agent's ability to identify and control a threat in its environment reflects its ability to complete the defensive cycle. The agent is supposed to be capable of influencing other agents' production, both directly and indirectly, in addition to the IDS domain. The combination of each demonstrates the shared indirect issues that agents encounter, whereas each focuses on direct manufacturing challenges. (Coulter and Pan. 2018).

**CHAPTER FOUR**

**4.0 APPLICATIONS**

Security is the top priority of IOT devices both currently in use or under development. IoT applications are fast growing and most of the present sectors have adopted it. Some of these IoT applications need strict security support from IoT-based technologies before it can work perfectly this will help the operators support of these apps effective with the current networking technology. there are various important IoT applications cutting across different sectors today.

**4.1. Home Automation**

IoT applications are numerous as it is used to automate house processes. It is categorized as applications for remote control electrical appliances to save energy, devices can be put on doors and windows to find intruders, and other activities too can be performed. The use of Energy and water is tracked through monitoring devices, and customers are being counseled on ways to conserve resources and money. (Jose & Malekian ,2017).

**4.2. Smart Cities**

Smart cities leverage newly available computing and communication technologies to better the lives of their residents (Lin et al. 2017). This includes Smart cities, smart transportation, smart disaster response, and other smart services. Governments across the globe are encouraging the creation of smart cities through different incentives (Gharaibeh et al. 2017). Although smart apps are created or developed to enhance the quality of life for people, they can also be risky in terms of privacy. Citizens’ credit cards as a means for purchasing and information might not be secure when using smart card services. Smart mobility apps can expose where their users are located. Parents can be able to monitor their children with the use of mobile apps. the children might be in danger though, if these applications were hacked. (Lin et al, 2017.)

**4.3. Smart Retail**

IoT Applications are used in retail. Many applications have been created with the ability to track the temperature and humidity of inventory as it flows across the supply chain. Additionally, IoT may be used to increase warehouse filling by monitoring how goods are transported. Intelligent apps for shopping will also being helpful in assisting consumers based on their preferences, habits, and sensitivities to certain components, for instance. these applications are being developed as an augmented reality system that allows physical shops to experience internet buying has also been created. IoT applications deployed and used by retail firms have been hit with serious security concerns (Eckhoff & Wagner, 2018).

**4.4. Animal Farming and Smart Agriculture**

Monitoring Soil moisture and maintenance of selective watering where there are no proper rainfall or micro-climate conditions, controlling the temperature and humidity is the responsibility required by most of the smart farming practices which they do not cover. Making use of sophisticated features in agriculture may lead to higher yields and assist farmers in avoiding unnecessary expenses. However, fungi and other microbiological pollutants can be avoided through monitoring and controlling of humidity and temperature levels in different vegetable and grain production processes (Lin et al. 2017).

**4.5. Smart Grids and Smart Metering**

Smart meters are useful in Managing, monitoring, and measurements. It is the most common to use smart meters in smart grids where power is used for tracking and measurement. A smart metering system could be helpful when combatting people using power illegally. Storage tank is responsible for monitoring and cistern level monitoring which is a two further uses for smart meters. By adjusting the position of solar panels in the sky, smart meters may also be used to monitor and enhance the performance of solar energy facilities. Other applications of IoT include smart meters to monitor water pressure to measure the weight of items or in water transportation systems. however, Smart meters are suitable for cyberattacks and physical attacks in contrast to traditional meters, which can only be interfered with by physical means. Smart meters or advanced metering infrastructure (AMI) are designed to carry out additional tasks beyond the normal tracking of energy in use. A smart home area network (HAN) is used for connecting all household’s electrical appliances to a single smart meter which eight Security and Communication Networks may be used to monitor use and costs. Consumer or adversary intrusions into such systems may alter the acquired data, resulting in financial losses for users or service providers (Namboodiri et al. 2014)

**4.6. Smart Environment**

Forest fires is identified using IoT devices which help to monitor snow levels at high altitudes preventing it in landslides, detecting earthquakes, monitor pollution, and other things. the lives of humans and animals in these regions are important in this region and the use of IoT applications in these regions will be important as information from these applications can be used by government entities working in these domains. the result of a security breach in any IoT application area might be high in this situation, wrong alerts from this system may affect IoT applications. For instance, if the app starts incorrectly by identifying earthquakes, the government and companies may suffer financial damage to the wrong people on the other hand, the software fails to detect earthquakes property and lives may be lost. security flaws and data manipulation must be avoided in smart environment applications. (Kumar, et al 2017)

**4.7. Security and Emergencies**

Deploying various IoT applications in the security sector is a groundbreaking development. Without proper credentials, user is not allowed to gain access to the system based on the restriction placed by the application harmful gas leak detection in industrial or chemical companies is another use for this technology. There are different buildings where vital information is stored in computers. Protecting this sensitive information and items is possible with the use of security apps. They are built with nuclear power plants to meet, high levels of sensitivity, which may be of benefits of using IoT apps that monitor liquids. the repercussions of a security compromise in these apps might be dire (Eckhoff & Wagner, 2018)

**CHAPTER FIVE**

**5.0 CONCLUSIONS**

In conclusion, this analysis emphasizes the critical need for novel methods to address cybersecurity concerns in the IoT age. Intelligent agents appear as a possible option, with the ability to learn, adapt, and interact autonomously to combat cyber threats. Using ideas from the current literature on intrusion detection and artificial intelligence, this research presents a paradigm for modeling intrusion detection systems as intelligent agents in the IoT environment. The ramifications of this research go beyond theoretical concerns, with practical applications in different industries, including home automation, smart cities, retail, agriculture, and emergency response. New research and development efforts are important to enhance the effectiveness and scalability of intrusion detection systems based on intelligent agents within the IoT context. Also, attention must be paid to addressing security and privacy concerns to ensure the widespread adoption and success of IoT applications.

**REFERENCES**

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.

Armanfard, N., Reilly, J. P., & Komeili, M. (2016). Local feature selection for data classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(6), 1217–1227.

Bengio, Y., Courville, A., & Vincent, P. (2013). Representation learning: A review and new perspectives. IEEE Transactions on Pattern Analysis and Machine Intelligence, 35(8), 1798–1828.

Chen, H., Summerville, D. H., & Chen, Y. (2009). Two-stage decomposition of Snort rules towards efficient hardware implementation. In Proceedings of the 7th International Workshop on Design of Reliable Communication Networks (DRCN 2009) (pp. 359–366). IEEE.

Coulter, R., & Pan, L. (2018). Intelligent agents defending for an IoT world: A review. Computers & Security, 73, 439–458.

Dasgupta et al. (2020). Machine learning in cybersecurity: a comprehensive survey. Journal of Defense Modeling and Simulation, Research Gate, 1-50.

Desai, M. M., Desai, M. M., & Desai, M. M. (2015). Internet of Things: A survey. International Journal of Computer Science and Engineering (IJCSE), 3(7), 2786–2790.

Eckhoff, D., & Wagner, I. (2018). Privacy in the smart city—Applications, technologies, challenges, and solutions. IEEE Communications Surveys & Tutorials, 20(1), 489–516.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., et al. (2017). Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials, 19(4), 2456–2501.

Haque, M. J., Magld, K. W., & Hundewale, N. (2012). An intelligent approach for intrusion detection based on data mining techniques. In Proceedings of the 2012 International Conference on Multimedia Computing and Systems (ICMCS) (pp. 12–16). IEEE.

Hussain, F. (2017). Internet of Things: Building Blocks and Business Models. Springer.

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22.

Igbe, O., Darwish, I., & Saadawi, T. (2016). Distributed network layer security management using a multi-agent system. In 2016 IEEE Symposium on Computers and Communication (ISCC) (pp. 917–922). IEEE.

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on the internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125–1142.

Lin, S.-W., Ying, K.-C., Lee, C.-Y., & Lee, Z.-J. (2012). An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection. Applied Soft Computing, 12(10), 3285–3290.

Lin, W.-C., Ke, S.-W., & Tsai, C.-F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-Based Systems, 78, 13–21.

Lugo-Cordero, H.M., & Guha, R.K. (2013). What defines an intruder? An intelligent approach. 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 31-36.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42–57.

Namboodiri, V., Aravinthan, V., Mohapatra, S. N., Karimi, B., & Jewell, W. (n.d.). Toward a secure wireless-based home area.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by the Internet of Things. Transactions on Emerging Telecommunications Technologies, 25(1), 81–93.

Rivera, J., & van der Meulen, R. (2015). Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. Gartner Newsroom.

Russell, S. J., Norvig, P., Canny, J. F., Malik, J. M., & Edwards, D. D. (2003). Artificial intelligence: A modern approach, vol. 2. Prentice Hall.

Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2011). Practical real-time intrusion detection using machine learning approaches. Computer Communications, 34(18), 2227–2235.

Sharma, A., Singh, P. K., & Kumar, Y. (2020). An integrated fire detection system using IoT and image processing techniques for smart cities. Sustainable Cities and Society, 61, Article ID 102332.

Sobh, T. S. (2006). Efficient signature discovery for intrusion detection systems. In The 4th ACS/IEEE International Conference on Computer Systems and Applications (pp. 1–8).

Sreelaja, N. K., & Pai, G. V. (2014). Stream-based random wireless sensor network using ant optimization and distributed agents for securing IoT-enabled environments. International Journal of Communication Networks and Information Security (IJCNIS), 6(2).

Stankovic, J. A. (2014). Research directions for the Internet of Things. IEEE Internet of Things Journal, 1(1), 3–9.

Tsai, C.-F., & Lin, C.-Y. (2010). A triangle area based nearest neighbors approach to intrusion detection. Pattern Recognition, 43(1), 222–229.

Wu, S. X., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing, 10(1), 1–35.

Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32.

Fang X, Liu L. Integrating artificial intelligence into Snort IDS. In: Intelligent Systems and Applications (ISA), 2011 3rd international workshop on. 2011. p. 1–4.

Jose, A. C., & Malekian, R. (2017). Improving smart home security: Integrating logical sensing into smart home. IEEE Sensors Journal, 17(13), 4269–4286.

Namboodiri, V., Aravinthan, V., Mohapatra, S. N., Karimi, B., & Jewell, W. (2014). Toward a secure wireless-based home area network for metering in smart grids. IEEE Systems Journal, 8(2), 509–520.

Kumar, S., Sahoo, S., Mahapatra, A., Swain, A. K., & Mahapatra, K. K. (2017, December). Security enhancements to system on chip devices for IoT perception layer. In Proceedings of the IEEE International Symposium on Nanoelectronic and Information Systems (iNIS) (pp. 151–156). Bhopal,