Volume 9, Issue 6, June – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN677

Advancing IOT Security: A Systemic and Cognitive Framework for Military Application

Mohamed Bahar
CSE Department, SOCSE
Sandip University, Nashik, India

Dr. Muhammad Muqeem; Dr. Omkar Pattnaik
Professor of Computer Science and Engineering
Sandip University, Nashik, India

Dr. Pawan Baldhare
Head of Department (HOD), at School of Computer Science and Engineering Sandip University, Nashik India

Abstract:- In the coming years, the protection of data, objects, networks, systems, and individuals within the Internet of Things (IoT) will take center stage in research and standardization efforts. The extensive connectivity of smart objects, coupled with their significant limitations, gives rise to numerous security issues that are not addressed by traditional security problem formulations and solutions. This work presents an overview of an IoT security roadmap to guide researchers interested in this field, based on a unique systemic and cognitive perspective. The function of each element of this approach will be clarified, and its relationships with other components and their influence on the entire system will be elaborated. In line with the innovative classification of IoT vision, a case study involving a military live simulation will be showcased to underline the components and interactions of the systemic and cognitive method. Following this, a discussionon security concerns related to privacy, trust, identification, and access control will be conducted, and various research challenges will be underscored.

Keywords:- *Internet of Things, Security, Systemic and Cognitive Approach, Military Live Simulation.*

I. INTRODUCTION

The Internet of Things (IoT) paradigm is designed to connect everything and everyone, anywhere and at any time This system integrates internet of things components and facilitating a smooth interplay between the tangible and virtual realms. By 2020, it is anticipated that The count of linked systems is projected to touch the mark of 24 billion units and the financial market size for mobile network operators across various sectors such as healthcare, transportation, public services, and electronics will be around 1.3 trillion dollars.

The transition from Transitioning from networks with limited access to those that are freely accessible. has amplified the need for security measures to safeguard interconnected devices from intrusions like data alteration, deletion, eavesdropping, Distributed Denial ofService DDoS, and other threats. Therefore, several complex Concerns related to safeguarding measures, including trust, security, and privacy, must be tackled before the IoT vision can be fully realized. This work makes three major contributions. The transition from networks with controlled access to those that are openly accessible. in the (IoT) has revolutionized the way military operations are conducted, offering improved effectiveness, surveillance, and responsiveness. However,this increased connectivity also introduces numerous security challenges. To address these challenges, A structured and thought-based approach is crucial for enhancing the security of IoT in military applications.

II. RELATED WORK

In scholarly works, numerous studies focus on remote monitoring systems, particularly in the fields of medicine and military. Here are summaries of some key studies:Shnayder and colleagues developed a remote monitoring system named Code Blue. This system uses a set of sensorsto monitor health parameters. It comprises three units: a finger-wearable pulse oximeter sensor that measures the patient's heart rate and blood oxygen level, an ECG board sensor that provides the cardiograph, and an EMG sensor that determines the patient's location and position. Milenkovic A. and colleagues utilized Wireless Personal Area Network and WBAN, during an emergency transfer, apatient's critical health information is sent to the hospital at regular intervals. Live data can be utilized for instant actions for the patient in transit and to arrange the required facilities in the hospital for swift diagnosis and recuperation. Baker C. and colleagues conducted a study to assess a patient's health conditions using data from Wireless Sensor Network nodes Situated in their residences or on their person, the body- attached nodes reveal their sleep/wake cycles and resting postures. Vital statistics like pulse rates and electrocardiograms can be observed from a distance throughsensors positioned on the patients' clothing. Concurrently, another research project successfully established a system for monitoring health in real-time using WSN communication infrastructure to track people's movements and locations indoorsThe system employs Monte Carlo localization algorithms, an accelerometer, and indoor mapping data to track individuals' step counts, locations, and movements. A team including Sevin A., Bayılmış C., and others developed an Emergency Discovery and Saving System using WSN nodes to tackle situations where a person falls overboard. In the maritime sector, such incidents are a major concern that can only be addressed by real-time

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN677

location tracking systems. In cases where a person falls overboard, the location of the victim is highlighted, especially when the incident happens in low light conditions.

In a separate study, a web-based application was created to monitor individuals' health metrics using WBAN technologies. The system offers a wide range of real-time monitoring services, particularly for the elderly and patients. Sensors placed on specific parts of their bodies record metrics like heart rate, blood pressure, and body temperature.This data is consistently logged in a database, allowingcaregivers to monitor and assess the conditions throughvarious interfaces on desktop or mobile platforms.

Ersoy C., and Alemdar H., conducted a review of numerous health service applications using WSNs. They divided the subject into three categories: locationtracking, activity detection, and medical status monitoring.

III. METHODOLOGY

This paper presents a comprehensive and systemic perspectiveIn the realm of internet of things, a structured and thought- based strategy is proposed to tackle the challenges and concerns related to IoT security. The recommended approach takes its initial inspiration from [5], where L. Kiely and team have presented a systemic security management system that can be applied to organizations of all types, beginning at the micro level. As shown in figure 1, our depiction of the IoT scenario is characterized by a model in the shape of a tetrahedron, constructed around four nodes: the individual, the process, the intelligent object, and the technological ecosystem. These nodes are linked, and their interplay isrepresented by the subsequent connections: trust, privacy,identification and access control, safety, reliability, auto immunity, and responsibility.

A. *Nodes*

The systemic and cognitive approach for IoT security is made up of four nodes:

- *Person*
- *Process*
- *Technology*
- *Intelligent Object*

Every node must collaborate to ensure consistency in the design and execution of secure applications. These interconnections among nodes are referred to as tensions. There exist seven types of tensions between nodes: identification, trust, privacy, reliability, responsibility, safety, and auto-immunity.

- *People:*

- Security issues are influenced by individuals' interests and actions, whether they are intentional or unintentional. People are responsible for carrying out tasksassociated with security management, which include:
- Formulating security practices and regulations tocreate effective security policy documents
- Evaluating the effectiveness of security practices and regulations, encompassing personnel, documentation,and technical control procedures
- Applying these practices and regulations in anoperational setting.

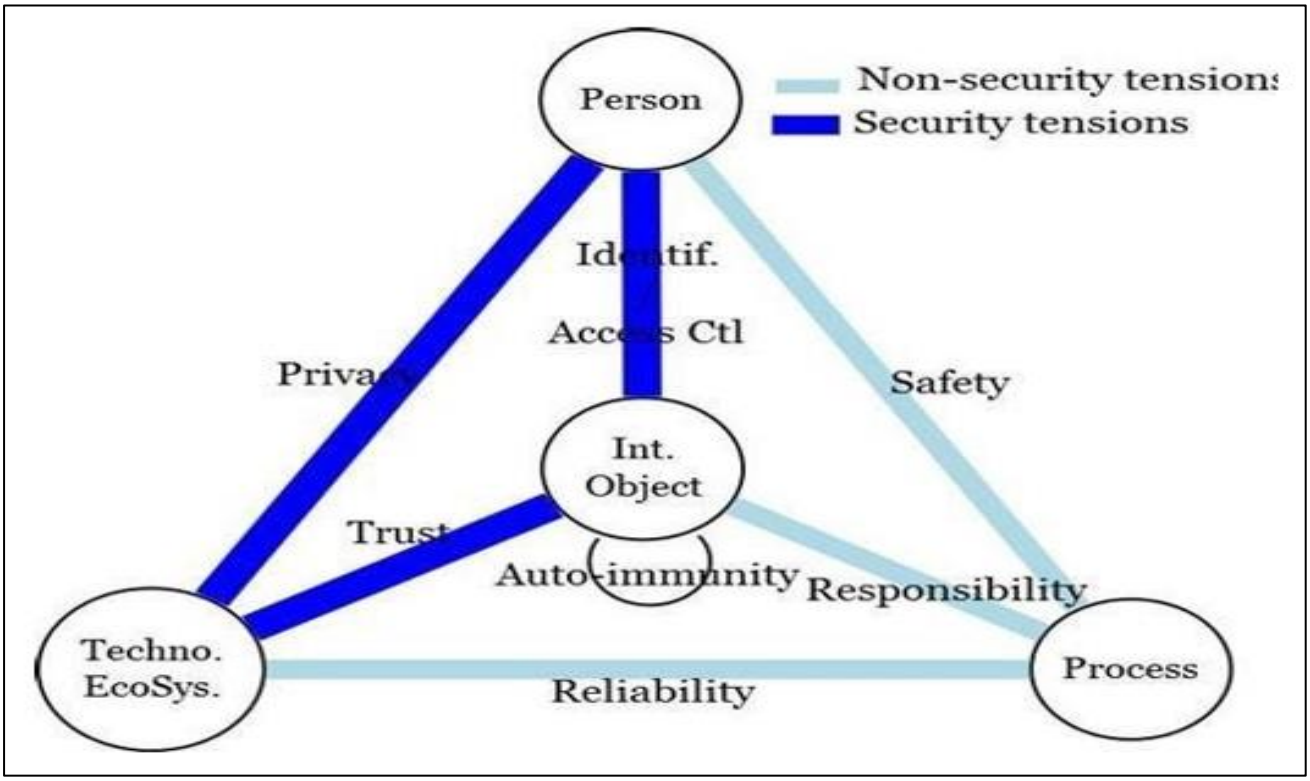

Fig 1: IOT Context Based on its Primary Components(Nodes) and their Interconnections(Edges)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN677

➢ *Process:*

The process needs to adhere to robust securitypolicies to maintain a satisfactory degree of protection. across various layers of the IoT architecture. The Federal Financial Institutions Examination Council has outlined a series of standard areas to be considered whenexecuting a secure process:

- Evaluation of Information Security Risks
- Formulation of Information Security Strategy
- Implementation of Security Controls
- Monitoring of Security Measures
- Review and Update of Security Processes

A secure process must comprehensively align with the requirements of policies, standards, strategies, procedures, and other specific documents or regulations.

➢ *Intelligent Entity:*

This node signifies an entity such asa sensory node (like a camera or X-ray device) or an RFID reader or tag (which identifies the existence of a person, animal, or object) that is part of a specific application.

➢ *Technological:*

This node pertains to the technological options that ensure a satisfactory level of IoT security. There are five classifications of information security components:

- Design and Configuration of Security
- Identification and Authorization
- Internal Enclave
- Boundary of Enclave
- Physical and Environmental Factors

B. Tension

➢ *Privacy:*

Privacy pertains to the strain resulting from the interaction between an individual and the technological ecosystem. Since safeguarded data is associated with humans, ensuring their privacy is a crucial goal of IoT. Privacy can be segmented into several areas, such as:

- Privacy during data gathering
- Privacy during data dissemination
- Privacy in data sharing and administration
- Issues related to data security

➢ *Trust:*

In the technological ecosystem, trust serves as the connecting bridge between the intelligent object and thesystem itself. The definition and operations of trust management are of significant importance, encompassing the establishment, updating, and revocation of credentials,keys, and certificates. However, in the context of the Internet of Things (IoT), there are substantial resource limitations and challenging technical decisions to be made.

➢ *Identification:*

Recognizing a specific object is acore issue that impacts the overall operation of the system,encompassing aspects such as architecture, components, and access rights.

➢ *Reliability:*

This strain can be considered when dealing with the addresses of unique and dependable entities, managing data across the network, or utilizing a device (or devices) efficiently for particular applications.

➢ *Safety:*

The extensive adoption of autonomous systems has sparked new concerns about their control software, whichcan exhibit erratic or unforeseen behaviour. Such circumstances need to be managed to prevent catastrophic outcomes for both the system and the broader environment. Individuals might also opt out due to issues related to privacy or safety, underscoring the critical importance of safety measures.

➢ *Responsibility:*

Responsibility is intricately linked to access permissions or authorization privileges. For example, if an IoT object is set up by a specific entity, it must manage connections from other objects and differentiate their varying access rights.

➢ *Auto-Immunity:*

Often, nodes are deployed in remote and challenging locations. As a result of locationlimitations, they become vulnerable and susceptible to physical attacks, necessitating the implementation of protective measures.

IV. PROPOSED WORK

To underscore the practicality of the advanced internet of things security approach, let's take the example of a military live simulation. In reality, Consider the scenario of a real-time military simulation. In actuality, operationalteams face a real adversary in a physical setting. simulations play a crucial role in their operational readiness. This implies that real individuals operate actual instrumented systems, with only the effects of weapons being simulated. These exercises will impact every subgroup, integrate actions of shots and manoeuvres, and unveil the skills of the leader. The replay and post-action review of the choices and individual performances of the actors also serve as a valuable lesson for optimizing the actors' actions. In this context, the nodes of the tetrahedron represent the following actors involved in the live simulation:

- **Identification:** This involves managing unauthorized intrusions of individuals or objects into restricted zones. It could include identifying and locating artillery and weapons, measuring explosives and harmful chemicals, tracking soldiers, detecting snipers, and managing surveillance parameters in sensitive areas.
- **Reliability:** This is cantered on the dependability of the Data collected and outcomes relayed by the technological ecosystem during the military manoeuvre. For example, if the simulators fail to induce the same level of stress as actual warfare, it questions the dependability of a virtual

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN677

simulation. becomes uncertain, as humans react differentlyunder stress. Moreover, equipment or vehicles may occasionally fail because unreliability was not accurately simulated. To address this issue, the behaviour of simulated equipment could model work failure, oil consumption, or ammunition usage based on values derived from actualexercises

- **Safety:** This strives to cater to the needs of intelligent objects,ensure their safety throughout their life cycle, and enhance personal safety by reducing injuries and fatalities during exercises. In defence operations, an adversary could exploit a medical device's vulnerability, such as cardiac pacemakers or diabetic pumps, resulting in the death of victims. Monitoring systems could facilitate an efficient health system and/or provide necessary health services.

In terms of privacy concerns, it is beneficial to implement applications that adhere to the data minimization principle to decrease the volume of personal data gathered and stored within IoT systems. Furthermore, innovative solutions can be devised to assist individuals in managing their own privacy settings and mechanisms, rather than relying on the internet of things system to fulfil their requirements. One potential solution involves utilizing Utilizing game theory for the representation of privacy administration by data proprietors.

Enhancements in recognition within the IoT framework can occur at multiple stages. A thorough identification system could be developed to aid individuals in navigating through numerous identification systems, especially when the hierarchical naming system employed on the Internet seems inappropriate for a diverse and highly mobile setting. Furthermore, the compatibility problem that arises when industries use proprietary standards for entity recognition needs to be tackled and resolved. Another issue is the establishment of a new infrastructure that uses distinct, non-overlapping addresses in dynamic and varied networks.

Mechanisms for access control, encompassing authentication and credential management, hold supreme significance in IoT.

V. RESULTS ANALYSIS

The analysis results from the paper showcased advancing internet of things (a systemic and cognitive framework for military application), It concentrate on the systemic and cognitive perspective for IoT security, specifically in the settingof military live simulation. Here are the primary insights:

- Systemic and Cognitive Perspective: The paper presents aninnovative methodology for IoT security that integrates systemicthought and cognitive elements, with the goal of tackling the intricate difficulties in safeguarding interconnected IoT devices.
- Military Live Simulation: A practical example involving a real-time military simulation is used to demonstrate the implementation of the structured and cognitive approach., demonstrating its potential in comprehending and addressing security issues in a practical context.
- Security Challenges: The paper discusses various security challenges in IoT, such as privacy, trust, identification, access control, and the need for a holistic security management system.
- Research Directions: It highlights several open research issues in IoT security, suggesting areas for future work, including privacy management, identification schemes, access control mechanisms, and trust models in heterogeneous networks.

VI. COMPARATIVE STUDY

A systematic and cognitive approach to IoT security, illustrated through a case study of military simulation and security challenges. Here are some key points from recent comparative research:

The pervasive nature of IoT brings forth valid concerns about security issues and how to manage the diversity of user and application needs. This necessitates the creation of adaptive, context-aware security solutions. The omnipresence of objects promotes content sharing, whichin turn necessitates a heightened focus on security and privacy in a dynamic and diverse environment. In this study, we offered a comprehensive systemic and cognitiveview of IoT, encompassing four components. We have shown that by adopting our methodology, it is feasible to monitor and comprehend security challenges in a specificcontext.

VII. CONCLUSION AND FUTURE SCOPE

➢ *The Future Research Directions Suggested by the Paper are:*

- **Privacy**: Developing applications for data minimization in IoT systems and solutions for usersto manage their own privacy settings.
- **Identification**: Creating a global identification scheme for IoT and addressing interoperability issues caused by proprietary standards.
- **Access Control**: Implementing scalable access control mechanisms that support the mobility of users and objects in IoT.
- **Trust**: The development of a universal Formulation of trust in varied networks and the inception of trust mechanisms for evolving infrastructures. These domains strive to bolster IoTsecurity and tackle issues associated with the dynamic and varied nature of IoT settings.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN677

REFERENCES

[1]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Gener.Comput. Syst.*, vol. 29, no. 7, pp. 1645– 1660, 2013.

[2]. Y. Challal, "Securite de l'internet des objets : vers une approche cognitive et systemique," HDR, Universite de Technologie de Compiegne, 2012.

[3]. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for iot security," in *DCOSS*.IEEE, 2013, pp. 351–355.

[4]. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for IoT security," in *International Conference on Computing, Networking and Communications (ICNC 2014)*, Honolulu, United States, 2014, invited Paper.

[5]. L. Kiely and T. V. Benzel, Systemic security management," *IEEE Security and Privacy*, vol. 4, no. 6, pp. 74–77, 2006. [6] [Online]. Available: http://www.27000.org/ "Advancing IoT Security: A Systemic and Cognitive Framework for Military Applications"

[6]. K. Klair, K.-W. Chin, and R. Raad, "A survey and tutorial of rfid anti-collision protocols," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 3, pp. 400–421, 2010.

[7]. R. Acharya and K. Asha., "Data integrity and intrusion detection in wireless sensor networks," in *2008 16th IEEE International Conference on Networks*, Dec 2008, pp. 1–5.

[8]. J. Medeiros, E. F. Watson, J. S. C. II, and M. S. Manivannan, Eds., *Proceedings of the 30th conference on Winter simulation, WSC 1998, Washington DC, USA, December 13-16, 1998*. WSC, 1998. [Online]. Available: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5993

[9]. J. E. Hannay, O. M. Mevassvik, A. Skjeltorp, and K. Brathen, "Live, virtual, constructive (lvc) simulation for land operations training: Concept development & experimentation (cd&e)."

[10]. NATO Science and Technology Organization, 2014