DOI: 10.64290/bimagombe.v9i2A.1149

# A Survey of Architectural Model for the Cyber Security of Internet of Military Things (IoMT) Devices

Yakubu Solomon[1] and Boukari Souley[2]

[1]Department of Computer Science, Nigerian Army University Biu, Nigeria
[2]Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi, Nigeria

Corresponding Author: solomon.yakubu@naub.edu.ng

## ABSTRACT

The Internet of Military Things (IoMT) devices covers large range of devices that retain intelligent physical sensing and actuation capabilities through either virtual or cyber interfaces that are integrated into systems which are used in military operations and missions to provide situational awareness to troops. These devices include sensors, actuators, vehicles, robots, UAVs, wearable device, biometrics, munitions, armor, analytical devices and other smart technology. Although these devices and associated networks provide advantages to troops, it creates the downside of cyber security challenges with the potential threat that a malicious adversary might penetrate the networks and compromise, the devices, networks and classified information through its vulnerabilities along the layers of its architecture. He large number of these devices and the network through which they connect are the major targets for enemies and other cyber criminals. Over the years, various architectural design and models for IoMT have been proposed to help in curtailing the incident of cyber-physical attacks. The limitations of the IoMT device to support the implementation and enforcement of traditional security mechanism including the terrain the devices will be used offer fresh difficulty for the security of the military mission and the IoMT devices. These have led to serious researches in the domain of IoMT security especially using either machine learning (ML) or deep learning techniques and other technologies. This survey reviews existing architectural models and ML/DL based security model for IoMT devices. Also, a new architecture is proposed providing interface for various security policy implementations. Finally, the survey recommends the application of DL/ML in IoMT security by selecting suitable architectural models which are to be deployed across the layers of the network and the use of autonomic IoMT security models in military warfare and combat operations.

**Keywords:** Internet of Military Things, Sensing devices, Munitions, Cyber-physical, Wearables devices.

## INTRODUCTION

The invention of Internet of things (IoT) has changed the way autonomous systems operate and plays a significant effort in harnessing the efficacy of military operations and missions in the battlefield (Farooq & Zhu, 2017). Thus, introducing IoT to cyber warfare and security will greatly enhance the operations of both military and the armed forces. This has directed the military thinking into looking for ways to improve operations and create a new base for military operation using communication networks (Hung & Gartner, 2019). The military make inference by looking at the information obtained from data to plan different military missions and operations; thus, stakeholders in the defense domain are interested in the latest technologies to develop on its information processing technology including information collection and aggregation, transformation and transfer. In their research of Internet of Battlefield Things (IoBT) security framework, Sharma and

Johnsen (2021) revealed that Internet of Battle Things has contributed to the development and increase in coordinating various military operations and mission by improving the equipment and battlefield operations. It has reduced the challenges on the battlefield by resolving various issues within communication technologies and device diversity.The aggregated information (Intel) is mainly used for situational awareness and is very important in military operations during battlefield using IoMT platforms which become force multipliers (Katalin, 2018). Information Aggregation and Integration of digital signals from different IoMT devices represents one of the several critical difficulties facing the implementation of IoT solutions on a battlefield (Cameron, 2021).

The modern military missions occur in complex and dynamic ecosystem and the commanders have little time to estimate information and perform elaboration of operation plan and taking decision based on all valuable information. The introduction and implementation of IoT in the military sector has mitigated some of these challenges. The modern military equipment has large capacity for processing large quantum of data and also network capabilities (Zeng & Carter, 2015). These networks of systems are used for reconnaissance and provide facts about battle situation as well as supply of medical gears and logistics. However, there exist some doubts especially with regard to security and privacy of data. Traditional IoMT systems are generally inadequate because issues of high complexity of systems, the limited capability and resources of sensors or detectors, and unpredictability of communication networks especially in remote locations. There is room for further research in order to identify specific security challenges and recommend solutions. The invention of Internet of Things is comprised of various connection and different devices. In 2015, IEEE reported a promising trend in IoT that enhanced the acceptability of the technology. The activities of the militaries in the future would depend a lot on smart device and systems talking to each other and performing unaided, also referred to as the 'Internet of Military Things' and IoMT is a technology that will change the collection and analysis of information between networks and humans to support intelligent interactions during military missions (GlobalData, 2018).

Further, adoption of IoT in the military will aid in logistics and military supplies and as well as providing situational awareness. This will help military personnel on missions. Future IoT, thus, would need strong security indeed if it's on insulated networks as the stakes would be high with high-cost outfit and device performing through IoT (Al- Garadi et al., 2020). In IoT, cyberattacks could not only be used for disrupting processes but also for snooping and gathering information unauthorized, for purposes like the smart snipper, smart soldiers, etc. Indeed, a lot of the cyber security threats over the Internet would be applicable to IoT in one form or the other. Secure IoT is, therefore, of great importance. With the use of Internet of Things in military especially logistics delivery, management of weapons and other equipment and technological advancement the pattern of warfare will drastically change in the future (Yang. et al., 2018).

Machine learning is a software technology that can learn from data through experience. It combines both data and statistical tools to predict an output or outcome. Deep Learning models can be used to embed predictive intelligence and knowledge in IoT device(Husain et al., 2020). Machine/deep learning techniques offer a great opportunity that can help IoT devices to deduce useful features from data of any kind. More so, communication of IoT devices generates large

DOI: 10.64290/bimagombe.v9i2A.1149

amount of traffic data that has specific features and differ from conventional network devices and developed ensemble ML model can be used for larger and heterogeneous IoT ecosystem (Cvitić et al., 2021).

Al-Garadi et al. (2020) and Hussain et al. (2020) published surveys on various machine learning and deep learning methods that can be used for IoT security. However, the survey findings revealed that most architectural models are suitable only for security of civilian IoT ecosystem and does not take into account the dynamism of cyber-physical warfare in the IoMT where most variables will continuously change due to adversary attacks and the nature of devices.

Moreover, the few available researches in the area of IoMT security and attacks mitigation models were also deficient in curtailing attacks across the various IoMT layers due to, among other things, the heterogeneous nature of devices and data, the increase in attack surfaces and attack sophistication. For instance, a DL-based researches by Dehghantanha et al. (2017) using deep Eigen space to detect malware in IoMT through device Operational code, though recorded a high detection metrics but could not guarantee performance on real-time datasets. Additionally, findings by Alkanjr and Mahgoub (2023) using a deception-based scheme to secure IoBT, an alias for IoMT, only concentrated on eavesdropping and inference attacks. Prema et al. (2023) also proposed a novel robust malware detection model for IoBT devices using deep Eigen space learning. The model is a modification of Dehghantanha et al. (2017) but here sequences from operational code was used in detecting in IoMT. The research used an ensemble of SVM (for classifying lower-dimensional representation of traffic data into malware and non-malware), an Auto encoder to extract features from the network traffic data and CNN was also used for lower-dimensional feature extraction and representation of the network traffic data. However, the model could not differentiate between opcode from either a rogue or legitimate device.

Recent research by Ruthravigneshwaran and Aritha (2023) on IoMT security using trust and K-means Clustering algorithm on IoMT network to detect blackhole attacks recorded only low accuracy and low precision. This is partly affected by the level of effectiveness and efficacy of the ML models used on IoMT devices which are mainly determined by the nature as well as the feature of the IoMT datasets as well as the performance of the learning algorithm (Sarker et al., 2022).

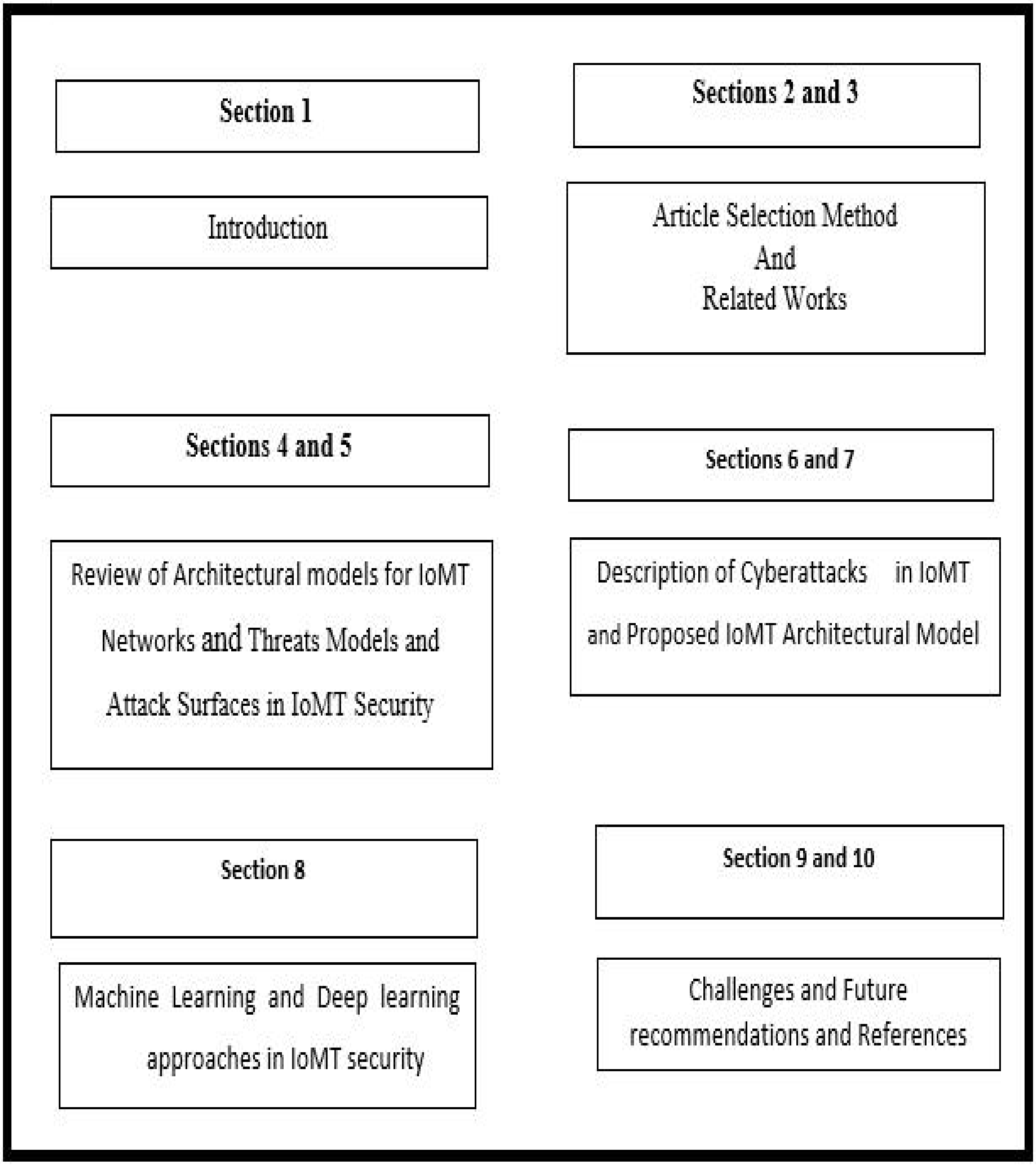
## Research Contribution

The following are the contributions of the survey

i. In-depth reviews of the cyber security architectural models of IoT and IoMT
ii. Provision of blueprint for adoption of IoT technology in the Military and Battlefield
iii. Design of novel architectural model for Cyber security of IoMT ecosystem
iv. Provision of baseline for the implementation of ML/DL base Cyber security frameworks for Internet of Military/Battlefield Things

DOI: 10.64290/bimagombe.v9i2A.1149

### Organisation of the Survey



Section 1

Introduction

Sections 2 and 3

Article Selection Method
And
Related Works

Sections 4 and 5

Review of Architectural models for IoMT Networks and Threats Models and Attack Surfaces in IoMT Security

Sections 6 and 7

Description of Cyberattacks in IoMT and Proposed IoMT Architectural Model

Section 8

Machine Learning and Deep learning approaches in IoMT security

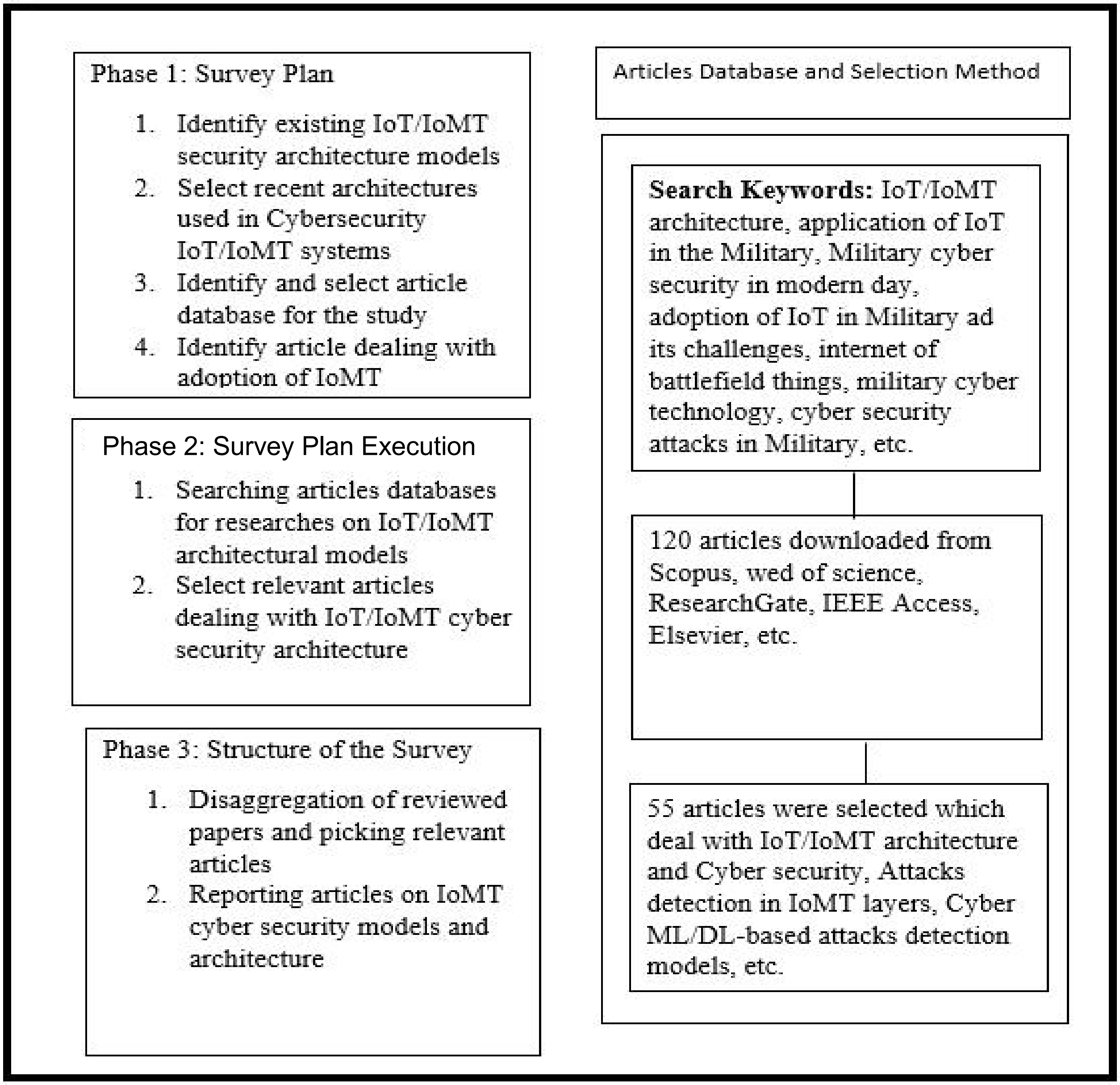
Section 9 and 10

Challenges and Future recommendations and References

DOI: 10.64290/bimagombe.v9i2A.1149

## Article Selection Strategy

The strategy employed in this survey is depicted in figure 1 below.



Phase 1: Survey Plan

1. Identify existing IoT/IoMT security architecture models
2. Select recent architectures used in Cybersecurity IoT/IoMT systems
3. Identify and select article database for the study
4. Identify article dealing with adoption of IoMT

Phase 2: Survey Plan Execution

1. Searching articles databases for researches on IoT/IoMT architectural models
2. Select relevant articles dealing with IoT/IoMT cyber security architecture

Phase 3: Structure of the Survey

1. Disaggregation of reviewed papers and picking relevant articles
2. Reporting articles on IoMT cyber security models and architecture

Articles Database and Selection Method

**Search Keywords:** IoT/IoMT architecture, application of IoT in the Military, Military cyber security in modern day, adoption of IoT in Military ad its challenges, internet of battlefield things, military cyber technology, cyber security attacks in Military, etc.

120 articles downloaded from Scopus, wed of science, ResearchGate, IEEE Access, Elsevier, etc.

55 articles were selected which deal with IoT/IoMT architecture and Cyber security, Attacks detection in IoMT layers, Cyber ML/DL-based attacks detection models, etc.

**Figure 1:** Survey Strategy

Inclusion criteria: Peer-reviewed articles, conference papers (2018-2024).
Exclusion criteria: Non-English, non-academic, irrelevant topics.

## RELATED WORKS

The IoT ecosystem is a big revolution due to the low prices of the devices but the size and magnitude of their memory makes difficult to fit in traditional security algorithms. Thus, lightweight encryption algorithms approaches have been the main mechanism before machine learning was developed. The use of lightweight encryption algorithms techniques

DOI: 10.64290/bimagombe.v9i2A.1149

became necessary because the IoT devices are not so big to offer the computational capacity required to achieve suck task. This has paved way for small and efficient algorithms in the IoT environment (Adwait et al., 2020). Studies have been conducted on the means and techniques of providing practical guide for existing security challenges in the IoT systems. However, these ML/DL studies were carried in a civilian IoT system where several things are under control unlike the IoMT. In his effort to provide solutions to cyber warfare, Zhu et al. (2018) stated that the focus of Internet of Military Things (IoMT) is to provide analytical data that will enhance situational awareness in military missions using the IoMT network. The US Army Research Laboratory's Tactical Network Assurance Branch developed an IoMT network in adversary locations for reconnaissance and communication. This was achieved using varieties of enhanced classification sensors. To preserve energy and power among devices and networks, robust sleeping algorithms were deployed. Also, Langleite et al. (2021) investigated the application of an IoMT subsystem limiting the architecture to an IoMT devices worn by personnel to help in improving combat effectiveness using enhanced surveillance systems. They further revealed that presently military missions and operations heavily rely on audiovisual communications for effective battle coordination between combat troops, logistics and command and control centers and these media are highly unreliable.

Bagaa et al. (2020) presented a new machine learning (ML) based security framework that dynamically and autonomously adapted to all aspects of IoT subsystem. This framework comprises of a mixture Software Defined Networking (SDN) and Network Function Virtualization (NFV) specifically designed to enhanced IoT attacks mitigation. This combination of approaches was highly successful in detecting the attacks with high accuracy and lower cost. Tawalbeh et al. (2020) explored the underlying security principles and policy by identifying security and privacy issues as well as approaches required to secure the IoT ecosystem. They proposed a novel IoT using layered architectural models comprising both privacy and security. Ibor et al. (2020) modeled cyberattack prediction using deep learning architecture to classify attacks in the system with rectified linear units (ReLU) as the activation function in the hidden layers and softmax function in the output layer of a Deep Neural Network (DNN).

Similarly, Askar et al. (2021) reviewed various autonomic techniques combined with deep learning and recorded god performance metrics. Syed et. al. (2020) proposed a DoS attack detection framework in the application layer for the MQTT protocol and recorded a high positive detection rate. Xiao et al. (2018) investigated ML-based attack mitigation model for the security of IoT. Bout et al. (2021) performed a survey on recent development in IoT security using ML for securing the IoT network infrastructure. They also provided detailed a description of how attacks based on the integration ML schemes are generated including majors features of the attacks and ML-based classification schemes. Kelton et al. (2019) studied relevant works that deal with several techniques related to intrusion detection architectures delving deeply in application of ML in IoT systems. Similarly, Kebande et al. (2020) examined the usage Real-Time Monitoring (RTM) to secure IoT system using surveillance for planning and mitigation of attacks in the cyber space. Radanliev et al. (2020) considered the real challenges in the use of machine learning in analysing the challenges of cyber security and its mitigation especially with regards to IoT networks and systems.

DOI: 10.64290/bimagombe.v9i2A.1149

Francesco et al. (2018) asserted that as the IoT will soon take over several human functions and will be available from globally and will be useful in addressing critical IoT security threats. Traditional techniques used against attack vectors were found to be insufficient. Thus, sophistication in cyberattacks will be about severe IoT/IoMT challenges which will require proactive approaches especially using ML-based autonomic approaches. Rajalakshmi et. al. (2020) provided a broader survey of works in the IoT security domain where ML based solution were implemented. The research shed light on different ML algorithms and models and other related functions. Sarker et al. (2021) presented a comprehensive view on cybersecurity implementation using AI techniques. Using the ML approach, Galán et al. (2022) using bibliometric approaches presented a ML model suitable for military IoT for analytics and inference which has a positive impact on the military cyber warfare. The advent of deep learning has also triggered so many studies in the application of deep learning models in the military domain. For instance, Dehghantanha et al. (2017) proposed a deep learning model comprising deep Eigen for IoBT security. The model was developed to detection malware through the device's operational code (Opcode) sequences. In addition, it successfully mitigated junk code insertion attacks.

Also, research by Zhu et al. (2018) proposed a constant checking of malformed data during information broadcast to guard against IoMT network from being flooded with irrelevant packets to cause DOS/DDOS. This was achieved by tuning down the XBee series radio's Personal Area Network (PAN) ID. If there was a suspected flooding of the network, the system switches to another network. The researchers also developed a sleeping algorithm to protect the IoMT devices from sleep deprivation. These measures were grossly inadequate due to duplication of attacks. In their simulation, a captured node was reprogrammed to send packet data nonstop to the command-and-control center in an attempt to jamb the network. This threat was countered by a packet threshold trigger resulting in all nodes switching off and their PAN IDs being dropped thereby restoring the network functionality and capacity. The research recorded high security metrics but increase in attack sophistication has rendered the mechanisms inadequate.

A study by Argin (2023) using a blockchain-based data security in military autonomous systems revealed a promising direction in increasing data integrity, authentication as well as resilient military autonomous systems against various threat models that significantly impede the success of military operations. Their study centered on authentication, integrity, availability, confidentiality and fault tolerance with encryption-based mechanisms developed.

Alkanjr and Mahgoub (2023) proposed an IoMT security mechanism using a deception-based scheme to secure IoBT nodes. They proposed an encryption mechanism coupled with dummy identities. A netlogo simulation was also developed. The design was made to hinder attacker vectors from obtaining location information (intrusion) from communication devices between IoBT nodes. The developed model effectively solved the threats of eavesdropping and inference attacks.

Recently, research by Rutravigneshwaran and Aritha (2023) into security of IoBT, an alias for IoMT, using trust and K-means clustering algorithm on the battlefield network have revealed the significant achievement of machine learning in IoMT security. The proposed model was used to detection blackhole attack in the network layer using CIC-2018 dataset and recorded some success.

DOI: 10.64290/bimagombe.v9i2A.1149

Alkanjr and Alshammari (2023) proposed an intrusion detection system (IDS) for IoMT that combines both unsupervised and supervised machine learning classifier to detect and report anomalies. In their approach, CIC-IDS-2017 and CIC-IDS-2018 datasets were used. The datasets were divided into the ratio of 70:30 for training and test.

Prema et al. (2023) also proposed a novel malware detection model for IoBT devices using deep Eigen space variant of deep learning. The model is a modification of Dehghantanha et al. (2017). However, in this model, the opcodes were first vectorized before the application of deep Eigen Space learning technique. In their setup, Eigen space components were used to boost sustainability and detection rates. A disassembler Objdump was used to extract the opcodes from the samples. The research used an ensemble of SVM (for classifying lower-dimensional representation of traffic data into malware and non-malware), an Auto encoder was used for feature extraction from the network traffic dataset whereas CNN was also applied in feature extraction from the lower-dimensional representation of the network traffic dataset.

## Review of Architectural models for IoMT Networks

The most fundamental structure of IoT is the architectural design and pattern ((Pal et al., 2019). Several researchers such Rachit et al. (2022); Mancini and Johnsen (2021) Tortonesi et al. (2020), Kudelski Group (2018); Pal et al. (2019); and Al-Garadi et al. (2020) have proposed various architectural design for IoT providing guiding principle for deployment, execution, maintenance and security. Rachit et al. (2022) states that the layered architecture provides comprehensive information and implementation of IoT based on the how IoT is characterized. In their design, the IoT is basically comprised of application interface layer, communication layer and the devices layer with each layer subdivide into various components. The application interface layer provides an avenue where devices connect together using interface modules like Arduino IDEA, Raspberry Pi, etc. The communication layer consists of switches and similar network units together with communication protocols and standards guiding IoT network traffic. The device layer composes of various interconnected components of the IoT network. However, the architectures proposed by both Pal et al. (2020) (Figure 2) and Said and Tolba (2021) (Figure 3) support the implementation of IoMT security. However, Pal et al. (2020) (Figure 2) provides a clearer and secured architectural approach that supports the implementation of secured IoT and thus can be modified and applied to IoMT security. They considered a five-layer functional architecture with each layer providing defenses to adversarial attacks of various vectors. Figure 1 shows the architecture proposed by Pal et al. (2020).

DOI: 10.64290/bimagombe.v9i2A.1149

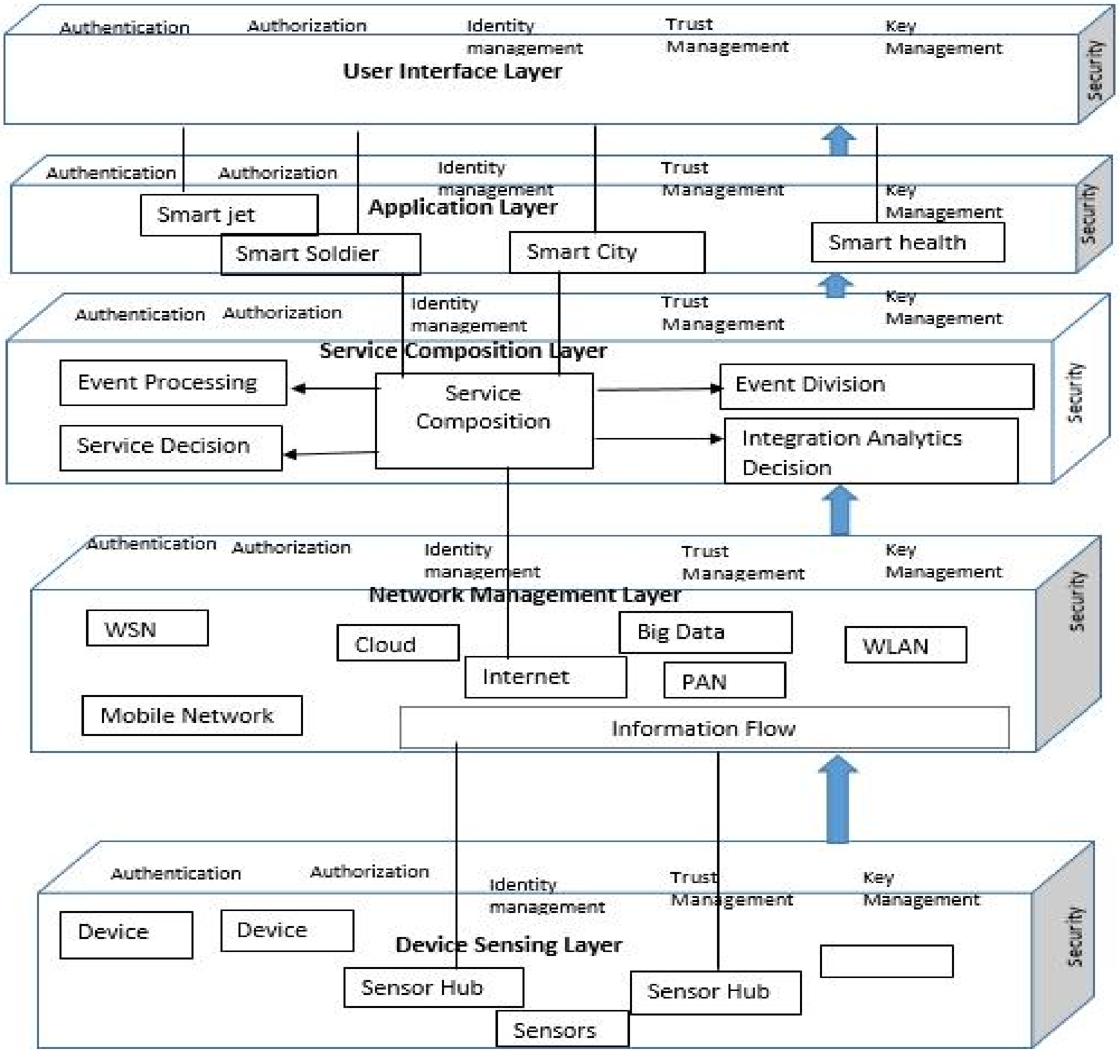


**Figure 2:** Layers of an IoT security architecture (Pal et al., 2020)

DOI: 10.64290/bimagombe.v9i2A.1149

**Table 1:** Summary of figure 1.

| S/No | IoT Layers | Core Components | Major Functionalities | Security Concerns |
|---|---|---|---|---|
| 1 | **Device Sensing** | sensing and actuating devices, RFID tags, etc. | For acquiring data from sensors and other network devices | Lack of authentication, proper authorization schemes and compromised access control interfaces |
| 2 | **Network Layer** | Communication media and devices, protocols and standards as well as cloud-based big data repository | For aggregating data and ensuring adherence to quality. | Lack of secure access and network devices compromise |
| 3 | **Service Composition Layer** | Middleware technologies and various objects | For data processing and analytics. | Lack of secure authentication schemes |
| 4 | **Application Layer** | Different applications like smart health, smart soldier, smart transportation, etc. | Setting messages protocol and standards | Compromised access, lack of privacy, etc. |
| 5 | **User Interface Layers** | End users and services | Deliver services and other functionalities to the end users | Lack of secure authentication, authorization and data adulteration |

DOI: 10.64290/bimagombe.v9i2A.1149

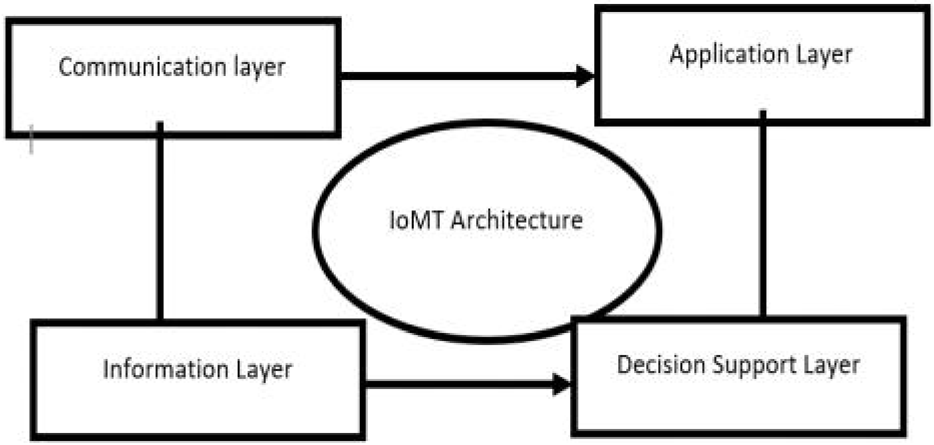


**Figure 3:** Simple view of IoMT architecture as proposed by Said and Tolba (2021)

Following the above architecture, Al-Garadi et. al. (2018) proposed a new three-layer architectural approach to IoT security with business objectives and Big data analytics. The architecture is shown in figure 4.

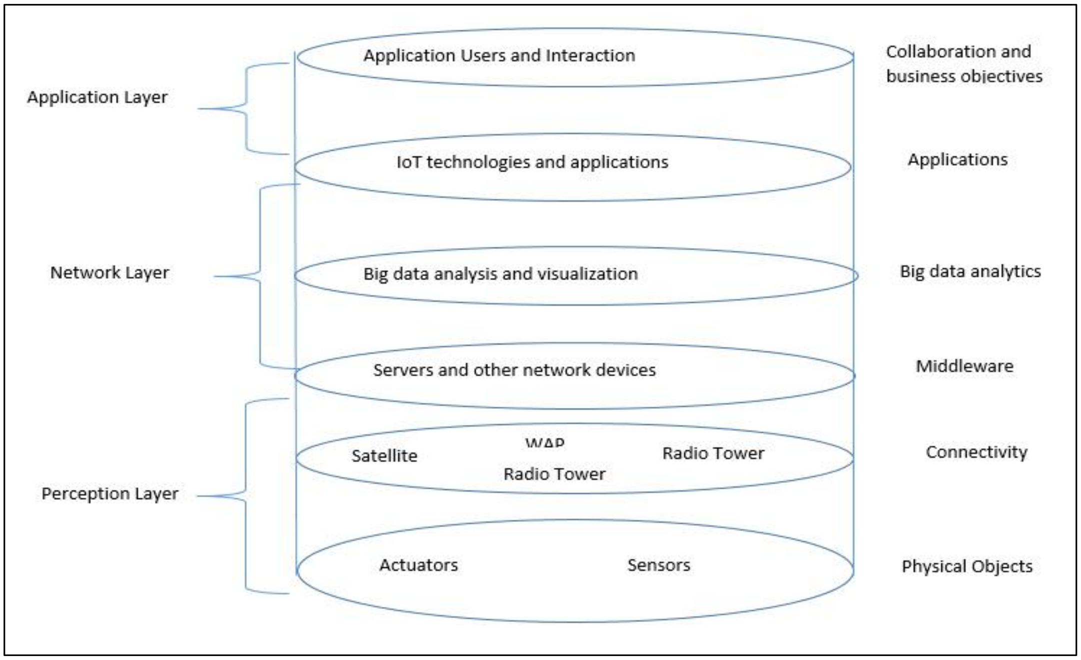

Application Layer
Network Layer
Perception Layer
Application Users and Interaction
IoT technologies and applications
Big data analysis and visualization
Servers and other network devices
Satellite
WAP
Radio Tower
Radio Tower
Actuators
Sensors
Collaboration and business objectives
Applications
Big data analytics
Middleware
Connectivity
Physical Objects

**Figure 4**: IoT architecture. Source: Al-Garadi et al. (2018.)

DOI: 10.64290/bimagombe.v9i2A.1149

**Table 2:** Summary of figure 2.

| S/No | Architectural Layers | Core Components | Major Functionalities |
|---|---|---|---|
| 1 | **physical Layer** | Sensing and actuating devices like muscle sensors, heart rate sensors, etc. | Sense and capture data from devices |
| 2 | **Network Layer** | Gateway, Router, Servers and other network devices. | Integrating sensors and other microservices. Provides big data analytics and middleware |
| 3 | **Application Layer** | Application and IoT technologies | it enables provides user interaction and collaborative business objectives. |

Similarly, Rachit (2020) proposed an IoT architecture shown in figure 5 below.

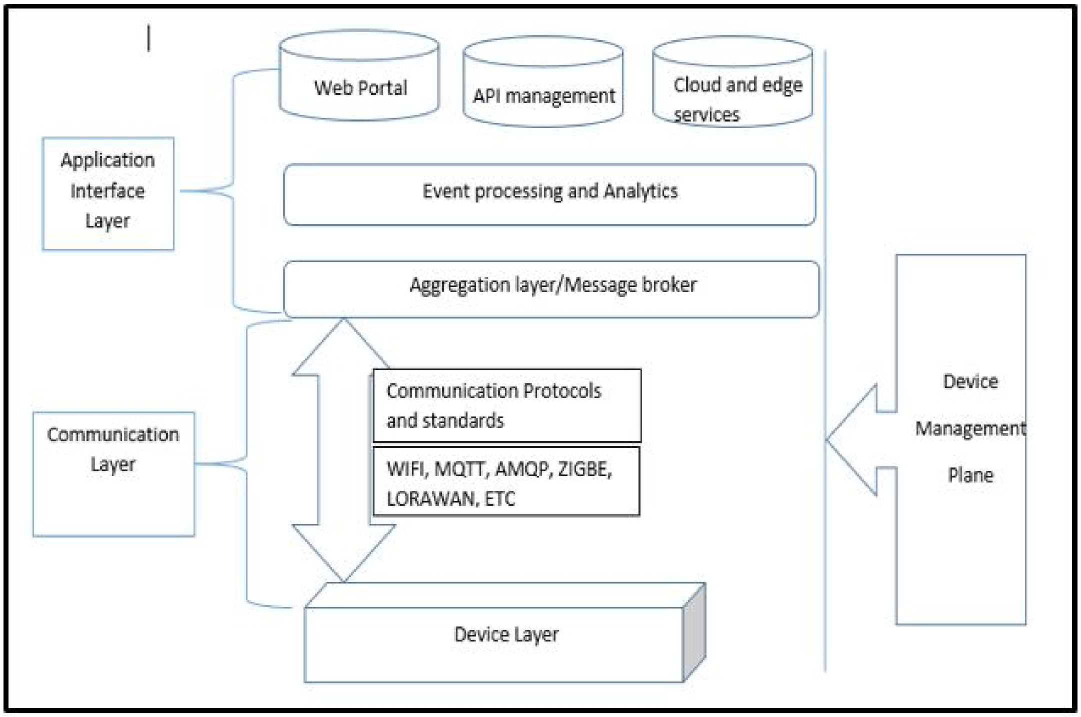

Web Portal
API management
Cloud and edge services
Application Interface Layer
Event processing and Analytics
Aggregation layer/Message broker
Communication Protocols and standards
WIFI, MQTT, AMQP, ZIGBE, LORAWAN, ETC
Communication Layer
Device Management Plane
Device Layer

**Figure 5:** Layered Internet of Things Architecture. Source: Rachit et. al. (2020).

DOI: 10.64290/bimagombe.v9i2A.1149

**Table 3:** Summary of figure 3.

| S/No | Architectural Layers | Core Components | Major Functionalities |
|---|---|---|---|
| 1 | Application Layer | Web portal, Application management, clod edge services, etc. | Event processing and analytics, aggregation and message brokering |
| 2 | Communication Layer | Networking units such as Switches and communication protocols and standard | General network connectivity |
| 3 | Device Layer | Arduino IDE, Raspberry pi, sensors, actuators, etc. | Sensing and data generation |
| 4 | Device Management Plane | Aggregator | Identification of data sources and destination. |

Said and Tolba (2021) considered architectural patterns of IoMT I relation to the security of devices shown in figure 4 below and the summary of its components and functionality is given in table 4.

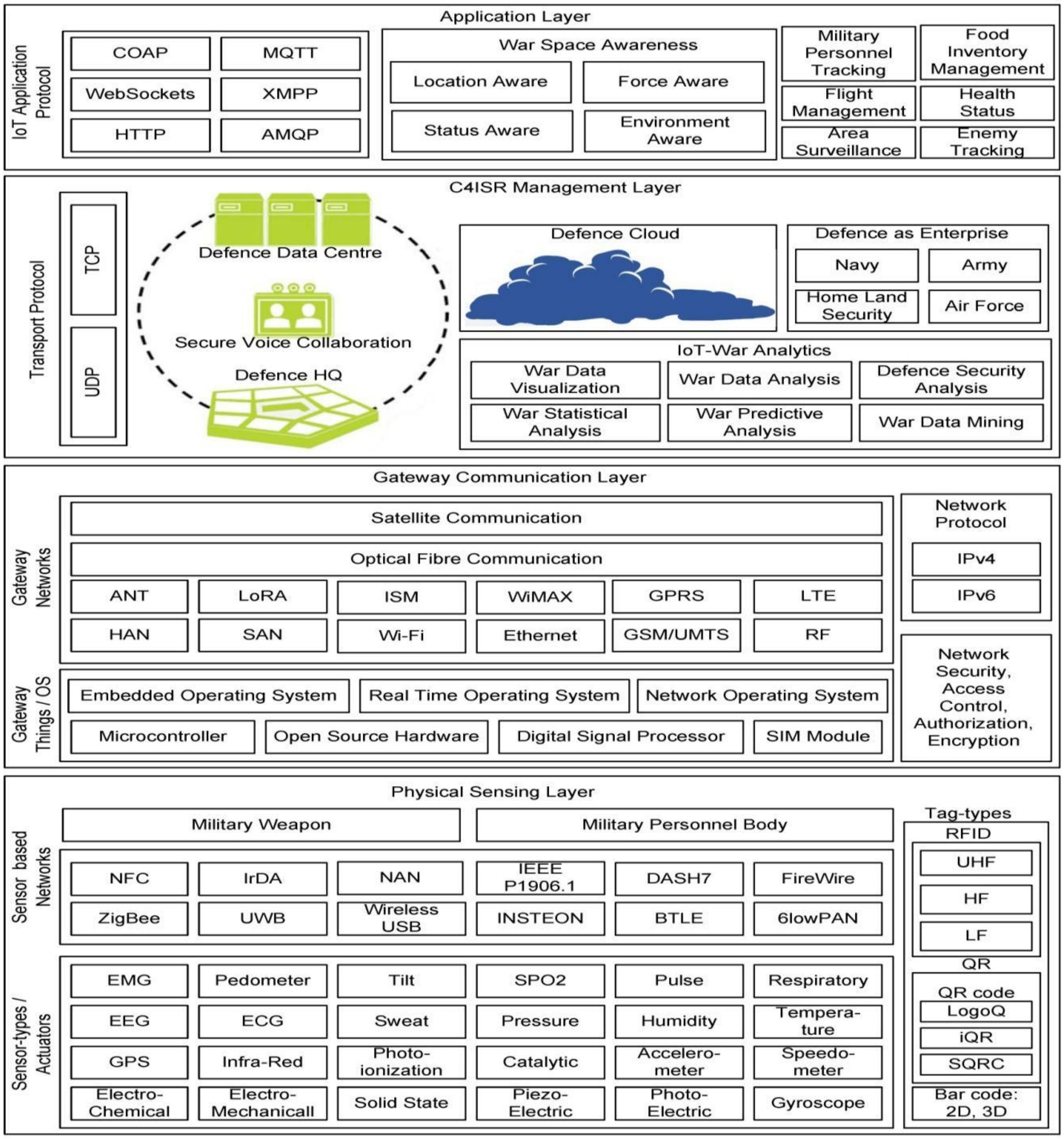
**Table 4:** Summary of figure 4.

| S/No | Architectural Layers | Core Components | Major Functionalities |
|---|---|---|---|
| 1 | Application Layer | Heterogeneous application and services | Provides user interaction and other service |
| 2 | Decision Support Layer | Middleware and software modules | Visualizing data analytics |
| 3 | Information Layer | Middleware | Transmission, storage and analysis of data in real-time |
| 4 | Communication Layer | Network and communication devices | Collection and delivering precarious data. |

Langleite et al. (2021) investigated the application of an IoMT subsystem limiting the architecture to an IoMT devices worn by personnel to help in improving combat effectiveness using enhanced surveillance systems. They further revealed that presently military missions and operations heavily rely on audiovisual communications for effective

DOI: 10.64290/bimagombe.v9i2A.1149

battle coordination between combat troops, logistics and command and control centers and these media are highly unreliable. The architecture proposed by these researchers is presented in figure 5.



Architectural framework of IoMT (Langleite et al., 2021)

DOI: 10.64290/bimagombe.v9i2A.1149

**Table 5:** The summary of the architecture.

| S/No | Architectural Layers | Core Components | Major Functionalities |
|---|---|---|---|
| 1 | Application Layer | IoT application Protocol and battlefield application | Provides user interaction and real time monitoring of personnel on battlefield |
| 2 | C4ISR Management Layer | Data repository and warehousing, mining and analytics | Data gathering, DHQ position and visualizing data analytics |
| 3 | Gateway and Communication Layer | Communication and network devices, network software modules | Transmission of long-range signals and network security controls |
| 4 | Physical Sensing Layer | Sensors and actuators, weapons fortified personnel body | Sensing of the environment and movement of devices across battlefield |

## Threats Models and Attack Surfaces in IoMT Security

The architecture of IoMT encourages various security threats due to exposure to large attack surfaces. The architectural design of IoT and hence IoMT provides a wide range of attack surfaces. The limitation in the capacity of IoMT devices and the domain they are used have made the susceptible to additional security challenges for both application and the devices. IoMT brings together connection and interaction for military missions by providing situational awareness (AL-Gharadi et al., 2020). In the case of the military, the primary military connections are military applications, military communication, military operations, logistics, drones and Unmanned Aerial Vehicle (UAVs) (Meneghello et al., 2019). Thus, securing the IoT system whether commercial or military is a complex task. Numerous threats such as passive attack(eavesdropping) and active threats (Spoofing, man-in-the-middle, Denial of Services (DOS), distributed DOS, etc.) might affect the IoT system (Al-Garadi et al., 2021). Although the IoMT connection is very crucial in facilitating activities of armed forces, it also suffers from serious security and privacy issues which are either active or passive. These security challenges consist of the following recon attack, node injection, man-in-the-middle, Node capture and distributed denial of service (DDoS) attacks. Hussain et al. (2020) further stated that due to large number of IoT devices that are deployed, the system has become increasingly threaten by attack vectors and therefore a more sophistication security solution modelmust be developed to defend against attack vectors. The taxonomy of attacks in the IoMT is shown in figure 5 below.

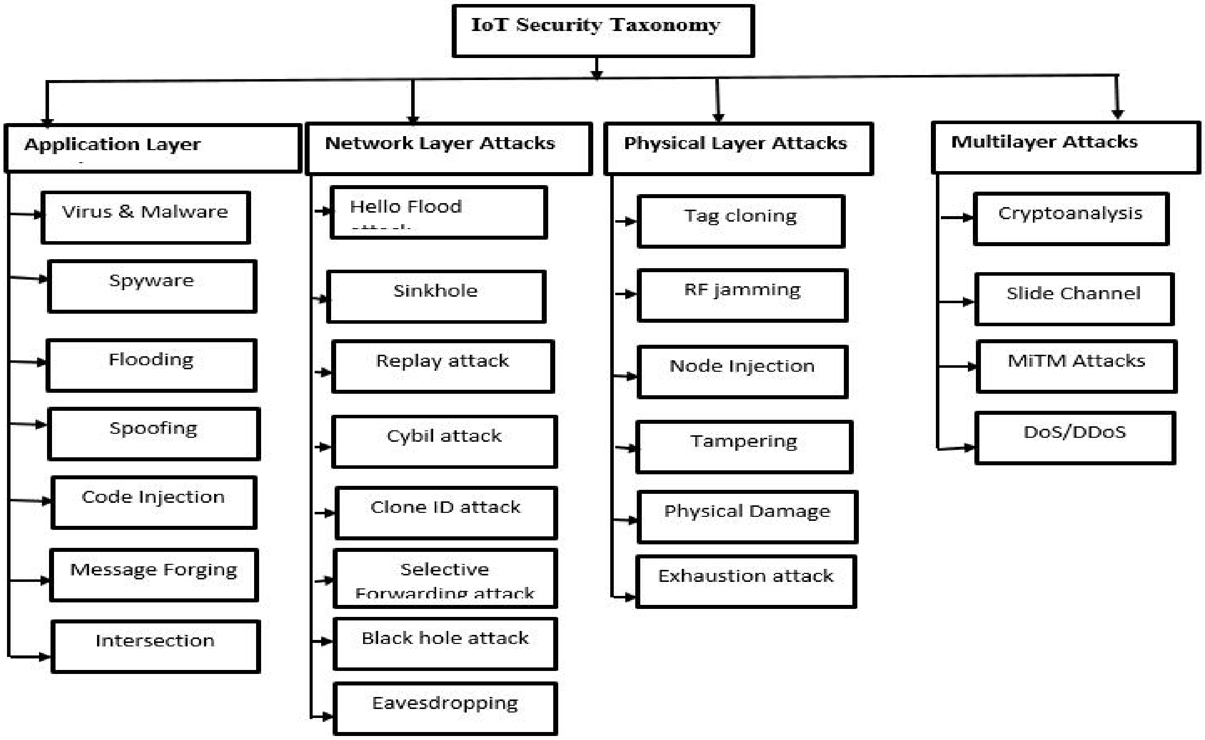


**Figure 6:** Taxonomy of IoT security attacks (Khanam et. al, 2017.)

### Description of Cyberattacks in IoMT

The various attack vectors prevalent in civilian IoT is also inherent in IoMT networks. The only difference is the types of devices affected by such attacks. Table 6 highlights the common cyber physical attacks militating against the success of both IoT and IoMT networks.

**Table 6:** Highlights the common cyber physical attacks militating against the success of both IoT and IoMT networks.

| Layer | Types of Attack | Intention | Mode of operation | Level of damage |
|---|---|---|---|---|
| Application | Virus &Malware | To compromise confidentiality of application in order to steal user credential and cause system shutdown | Attacks occur in the form of either worm, virus or trojan | Damages IoT devices and network technologies |
| | Spyware | to monitor the activities of user in order to steal credentials | Using installed applications or microservices | Harm devices, network resources and users |
| | Flooding attack | To exhaust node resources | By transmitting signals that are beyond the capacity of network devices and media | Lifespan of devices are shortened |
| | Spoofing | To hinder authentication and user privacy | Using node imitation or impersonation | Loss of confidentiality and trust |
| | Message forging | To compromise information integrity | By creating new fake messages or modify existing ones | Feed users with fake messages and compromise information integrity |
| | Code Injection | To insert a rogue node in order to steal authentication details | By inserting harmful codes or subroutine into application to hinder execution or retrieve information | unauthorized access to user’s accounts |
| | Intersection Attack | To disrupt the privacy of users | By planting itself in between nodes to harvest information from other devices | Can lead extensive attacks |
| Network | Hello Flood Attack | To change routing path | By violating routing protocols and creating new malicious route | Transmitting fake messages and drop legitimate one |

| | | | | |
|---|---|---|---|---|
| | Sinkhole Attack | To initiate multifaceted attacks | By denying to server devices | Complete network disruption |
| | Replay attack | To exhaust system and network resources | By resending packets across the network to exhaust resource | Complete network disruption |
| | Sybil Attack | To replace legitimate nodes with fake ones | By replicating IDs and intrude network systems | Packets will be dropped in transit |
| | Clone ID | To attach a device to the network with intention to steal information | By impersonating legitimate nodes in a network | Stealing user data |
| | Recon attack | To gather information about the network topology and security policies | By performing vulnerability assessment before launching attacks | Extensive attacks across all IoT layers |
| | Blackhole | To disrupt network operation | By making destination devices unreachable | Entire network disruption |
| | Eavesdropping and traffic analysis | To gather facts about a network preparatory to attack | By transmitting messages across the network and perform analysis of response | User privacy and confidentiality can be compromised |
| Physical | RF Jamming | To prevent network communication | By interfering with certain frequency range to disrupt radio frequency | Complete disruption of transmission frequency |
| | Tag Cloning | To insert imitation tags in a network | Through reverse reengineering | Siphon users' credential and cause serious financial loss |
| | Node Injection | To gain access to a network and transmit data or signal | By planting dubious nodes in the network | Locks out legitimate user from the network |
| | Tampering | To tamper with content of devices attached to a network | By physical damaging or disconnecting devices attached to | Deny users both availability and confidentiality of resources |

DOI: 10.64290/bimagombe.v9i2A.1149

| | | | | |
|---|---|---|---|---|
| | | | a network | |
| | Physical damage | To steal, break or willfully disconnect node or devices from a network | By physical stealing nodes | Complete disruption of the network |
| | Rogue device insertion | To conduct recon attack | By masquerading an illegal node as legitimate | Launch a devastating and extensive attack |
| Multi-layer Attacks | Side Channel Information Attack | To capture and analyse network information | By analysing non-network devices like power and other resources | Launch a devastating and extensive attack |
| | DOS | To disrupt network services | By overcrowding the network with dummies data or signal | Renders services unavailable to users with accompanying financial loss |
| | Cryptoanalysis | To break encrypted resources by decrypting keys. | By persistent trial and error techniques. | Decrypting secure messages and retrieve information. |

Source: Hussain et. al. (2020)

## Proposed IoMT Architectural Model

As stated earlier, the civilian IoT architectural model cannot adequately support the implementation of a secure IoMT. Thus, this survey proposes a secure IoMT architectural model shown in figure 7 below.

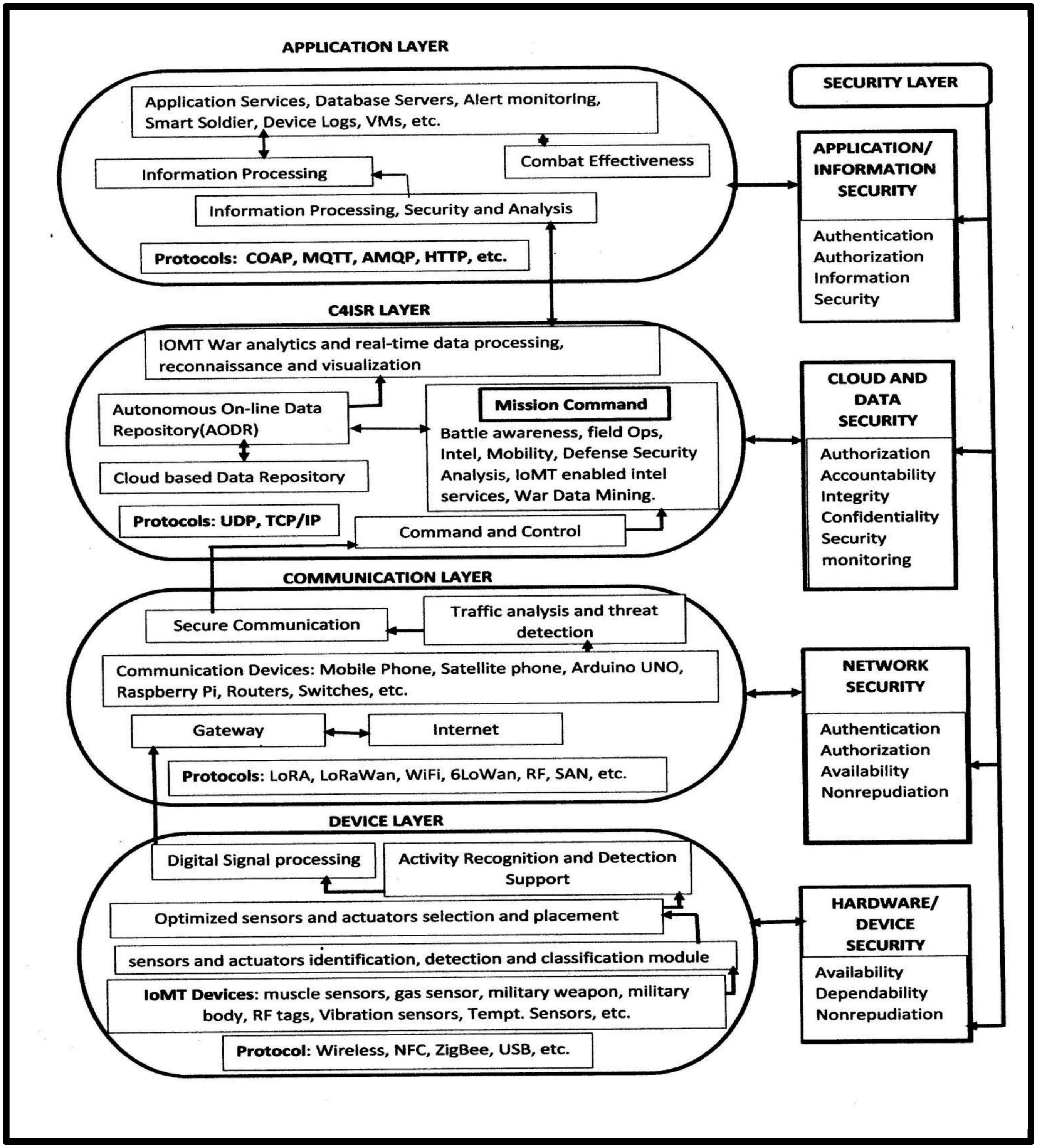

APPLICATION LAYER
Application Services, Database Servers, Alert monitoring, Smart Soldier, Device Logs, VMs, etc.
Information Processing
Combat Effectiveness
Information Processing, Security and Analysis
Protocols: COAP, MQTT, AMQP, HTTP, etc.
SECURITY LAYER
APPLICATION/ INFORMATION SECURITY
Authentication
Authorization
Information
Security
C4ISR LAYER
IOMT War analytics and real-time data processing, reconnaissance and visualization
Autonomous On-line Data Repository(AODR)
Mission Command
Battle awareness, field Ops, Intel, Mobility, Defense Security Analysis, IoMT enabled intel services, War Data Mining.
Cloud based Data Repository
Protocols: UDP, TCP/IP
Command and Control
CLOUD AND DATA SECURITY
Authorization
Accountability
Integrity
Confidentiality
Security
monitoring
COMMUNICATION LAYER
Secure Communication
Traffic analysis and threat detection
Communication Devices: Mobile Phone, Satellite phone, Arduino UNO, Raspberry Pi, Routers, Switches, etc.
Gateway
Internet
Protocols: LoRA, LoRaWan, WiFi, 6LoWan, RF, SAN, etc.
NETWORK SECURITY
Authentication
Authorization
Availability
Nonrepudiation
DEVICE LAYER
Digital Signal processing
Activity Recognition and Detection Support
Optimized sensors and actuators selection and placement
sensors and actuators identification, detection and classification module
IoMT Devices: muscle sensors, gas sensor, military weapon, military body, RF tags, Vibration sensors, Tempt. Sensors, etc.
Protocol: Wireless, NFC, ZigBee, USB, etc.
HARDWARE/ DEVICE SECURITY
Availability
Dependability
Nonrepudiation

**Figure 7:** Proposed IoMT architecture.

DOI: 10.64290/bimagombe.v9i2A.1149

## WORKING PRINCIPLE OF THE PROPOSED MODEL

### The Application Layer

This layer consists of various applications and services that used in military activities such as reconnaissance, cloud services, OS servers, management, surveillance, etc. The application layer of an IoMT is the most important aspect IoT subsystem, which provides an avenue where network and other software application interact. It provides a several functions like information and security processing services, presentation, monitoring of device conditions and logs, virtual machines, combat effectiveness interface, notifications or alert, device control functions, etc. Typically, this layer includes support for services and microservices and platform, middleware, servers, application services and computational software. Therefore, this layer provides most of the interfaces required for mission assessment and combat effectiveness. Protocols such as COAP, MQTT, AMQP etc. are being used in this layer. Also, this layer suffers from various threats such sniffing attack, access control attack, service interruption attack, malicious code injection, reprogram, cross site scripting attack etc.

### C4ISR Management Support Layer

The Command-and-Control layer also referred to as Command, Control, Communication, Cyber, Intelligence, Surveillance, and Reconnaissance (C4ISR) is the second layer after the application layer. This is where IoMT war analytics and real-time data processing takes place. It also supports and house a cloud-based data repository as well as an autonomous on-line data repository. Battle awareness, field operations, intel gathering, military personnel mobility, defence security analysis and war data mining are the key features of the mission command, a such layer in the C4ISR. The layer receives a secure communication containing encrypted information from the communication layer. The operations of this layer is govern by two protocols namely, UDP and TCP/IP. Signals received in this layer is warehoused, analyzed and interpreted by military heads and other stakeholders. The layer is however threatened by the following cyberattacks: DDOS/DOS, SQL code injection, Storage attack, eavesdropping, sniffing attacks, etc.

### The Communication Layer

The IoMT communication layer provides connectivity needed to connect sensors, actuator and other computing devices together. The communication layer of the IoMT proposed above serves a gateway to both physical layer (to be discussed shortly) and the C4ISR Management Support Layer. Utilizing variety of protocols, such as LORA, RPL, SAN, HAN, 6LOWAN, WIFI, ISM, RF, LTE, BLE, WSN, etc. this layer contains various network devices and software such as Real-time OS, Network OS, XBee Series 2, Raspberry Pi, Arduino UNO, Gateway, Bridges, etc. These components provide different functionalities. The Arduino UNO device is also used in this layer provide connectivity to several sensors and actuators as well as other modules module. Using the Raspberry Pi as the base station will enable all of the sensor data to be sent to a central database and it also offers more computing power than other devices and supports the execution of ML/DL algorithms. These sensors and actuator are connected to this layer via a gateway. Cyber threats common in this layer include phishing attack, DDOS, MITM, data transit attack, routing attack, exploit attack, etc.

DOI: 10.64290/bimagombe.v9i2A.1149

### *The Physical layer*

This layer includes physical world objects and virtual entities such Military Weapon, Military personnel body, Smart Phones, RFID tag, Microphone, Camera, RF, Vibration, IFF (friend or foe), Ultrasonic, PIR, Gas sensors, Muscle activity sensors, etc. They are used for data collection through sensors from devices in the ecosystem. Protocols embedded in this layer include NFC, IrDA, NAN, ZigBee, Wireless USB, etc. IoT devices are built with electromechanical modules and components such sensors, actuators, microprocessors and other body-worn devices that can aggregate, process, identify and store data in repositories. The sensors would the transform the dataset collect into binary format. IoT devices gather sensory data from the ecosystem such are heartbeat, location of adversaries, bullet count, etc. The sensors and actuators' detection and identification module provide an interface for integrating robust security mechanism for screening every device in the layer. RF jamming, physical damage, Tampering, tag cloning, node capture, side channel attack, booting attacks, malicious code injection and Collusion etc. constitute security challenges in the IoMT layer.

### *The Security Layer*

The security layer of the IoMT network is a layer dedicated for provision of security frameworks and policies that guarantees security, protection, provisioning, smooth operation and effectiveness of the overall architecture. The security layer oversees the security principles and requirement, confidentiality, authentication, monitoring and analytics, nonrepudiation, etc. A detailed description of the sub-security layers is given below.

### *Application security*

This layer is responsible for providing various security principles and requirements for both application and services. Security requirements such authentication, authorization, information security, user management and trust as well as privacy issues

### *Cloud and Data security*

Data security is very important in the CSISR layer. This is arguably the most important aspect of the ecosystem when it comes to war management. Any intrusion, malicious attack or false data injection will render an entire mission ineffective or disastrous. The issues of confidentiality, data integrity, authorization, authentication, security monitoring and analytics are provided in this sublayer.

### *Network Security*

The communication network security is the bedrock of IoMT. Digital signals and packets need to be safeguarded using state-of- the-art technologies. The identity of communicating devices needs to be authenticated. This is to ensure that certain devices have not been taken over by bots thereby compromising the entire IoMT network infrastructure. Nonrepudiation, availability, and authorization are key security principles to be enforced.

### *Device security*

The perception layer is the cradle for the IoMT configuration and design. Any acts capable of interfering with the smooth operation of the devices in the ecosystem will render it either useless or dangerous. An insertion of a rogue device in the device layer, node capture and physical damage will lead to a ripple of serious and multidimensional attack across the remaining layer in the architecture. The security requirements in this

DOI: 10.64290/bimagombe.v9i2A.1149

sublayer include availability, dependability, reliability, and maintainability.

### Machine Learning and Deep learning approaches in IoMT security

Al-Garadi et al. (2020) and Hussain et al. (2020) published surveys on ML/DL methods for the securing IoT systems. The surveys centered on ML based models such as Support Vector Machine (SVM), Random Forest, Decision Tree, K-Nearest Neighbour, etc. while deep learning models such as AutoEncoder, Generative Adversarial Network (GAN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) and Deep Neural Network (DNN) were also considered. The performance metrics for these models in IoT were also very encouraging. The survey however, concentrated on civilian IoT.

Presently, there are few available researches in the area of IoMT security and attacks mitigation models. Although some are effective others are deficient in curtailing attacks across the various IoMT layers due to, among other things, the heterogeneous nature of devices and data, the increase in attack surfaces and attack sophistication. Rajalakshmi et. al. (2020) provided a broader survey of works in the IoT security domain where ML based solution were implemented. The research shed light on different ML algorithms and models and other related functions. Sarker et al. (2021) presented a comprehensive view on cybersecurity implementation using AI techniques. Using the ML approach, Galán et. al. (2022) presented a machine learning model architecture that can be applied in military IoT, adopting techniques used in civilian domain and collected dataset were modeled and analyzed and concluded that the efficacy of ML in the military environment cannot be overemphasized. The advent of deep learning has also triggered a lot of studies in the application of deep learning models in the military domain. For instance, Dehghantanha et al. (2017) presented a deep Eigen space learning-based model for IoBT security. The model was developed to detection malware through the device's operational code (Opcode) sequences. In addition, it successfully mitigated junk code insertion attacks.

Researches into the detection of rogue devices inserted into network infrastructure have also been caried out by Yin et al. (2021) who developed a deep learning IoT device detection model consisting of CNN and BiLSTM. Their work was based on IoT device detection and classification irrespective of whether it was benign or rogue devices, passive or active. The developed model, called CBBI, was designed to identify different kinds of devices across an IoT. This approach was deployed to get information about different kinds of device and their categories on an IoT network. Similarly, Liu et al. (2020) presented a comprehensive survey on machine learning based model for detection and classification of IoT device highlighting major successes in this area. However, the survey revealed that classifying unknown device from the same manufacturers presented a big challenge using machine learning approaches. Further, the need for continual learning when a new and unknown IoT device is introduced into the IoT network was a is yet to be met (Yin et al., 2021), issues with reliable real-time benchmark datasets, performance assurability, detection and classification of an attacking device, imprinting verifiable patterns in IoT devices to evade adversary were the major difficulties left unattended during their works.

A study by Argin (2023) using a blockchain-based data security in military autonomous systems revealed a promising direction in

DOI: 10.64290/bimagombe.v9i2A.1149

increasing data integrity, authentication as well as resilient military autonomous systems against various threat models that significantly impede the success of military operations. Their study centered on authentication, integrity, availability, confidentiality and fault tolerance with encryption-based mechanisms developed.

Alkanjr and Mahgoub (2023) proposed an IoMT security mechanism using a deception-based scheme to secure IoBT nodes. They proposed an encryption mechanism coupled with dummy identities. The developed model was evaluated using a novel mathematical to identify real packets for each location information update. A simulation using netlogo was also developed. The design was made to mitigate attacker vectors' ability to obtain location information (intrusion) from the communication network between IoBT nodes. The developed model effectively solved the threats of eavesdropping and inference attacks.

Recently, research by Rutravigneshwaran and Aritha (2023) into security of IoBT, an alias for IoMT, using trust and K-means clustering algorithm on the battlefield network have revealed the significant achievement of machine learning in IoMT security. The proposed model was used to detection blackhole attack in the network layer using CIC-2018 dataset and recorded some success.

Alkanjr and Alshammari (2023) proposed an intrusion detection system (IDS) for IoMT that combines ensembles of supervised machine learning classifier with other unsupervised models to detect and report anomalies. In their approach, CIC-IDS-2017 and CIC-IDS-2018 datasets were used. The datasets were divided into the ratio of 70:30 for training and test.

Prema et al. (2023) also proposed a new malware detection model for IoBT devices using deep Eigen space variant of deep learning. The model is a modification of Dehghantanha et al. (2017) to detection malware in IoMT. However, in this model, the opcodes were first vectorized before the application of deep Eigen Space learning technique. In their setup, Eigen space components were used to boost sustainability and detection rates. Also, a disassembler Objdump was used for feature extraction of operation codes from the samples. The research used an ensemble of SVM (for classifying lower-dimensional representation of traffic data into malware and non-malware), an Auto encoder to extract features from the network traffic data and CNN was also use in the lower-dimensional representation feature extraction of the network traffic data.

## CONCLUSION

The review work carried has provided us with adequate knowledge for the adoption and deployment of DL/ML models in IoMT security. It can be concluded that the adoption and implementation of any security framework and policy in an IoMT network is dependent upon the architectural model adopted and that the application of such models should conform to operational guidelines provided by the Command-and-Control Centers who are responsible for the coordination of military missions and combat operation. Furthermore, the sophistication of the adversary, distance between Command-and-Control Centers and terrain determine the IoMT security protocol and technology to be deployed.

### Challenges and Future Recommendations

Due to increase in diversity and sophistication of cyberattacks the challenges of securing the IoMT ecosystem is still an active research area. It is generally difficult to design efficient and autonomous models that will patrol the IoMT network and detect, prevent and

DOI: 10.64290/bimagombe.v9i2A.1149

recover systems from adversary attacks. Proponents of artificial cyber hunters argue that adaptive autonomous models should be incorporated into the security architecture and designs of IoMT. More so, additional research into the construction of secure data storage and transmission methods as well as IoMT protocol for secure IoMT networks should be carried out.

## REFERENCES

Al-Garadi M. A., Mohamed A., Al-Ali. A. K. (2018). Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE journal.

Al-Garadi M. A., Mohamed A., Al-Ali A. K., Du X., Ali I. and Guizani M. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security, in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-168. doi: 10.1109/COMST.2020.2988293.

Angin P. (2020). Blockchain-based data security in military autonomous systems. International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) – 22-24. doi**:** 10.31590/ejosat.824196.

Adwait P., Tejas P., Shubham P., Piyush R. Smita K. (2020). A Survey on Methodologies for intensifying the security in IOT environment, Journal of critical reviews, 7(19).

Alkanjr B. and Alshammari T. (2023). IoBT intrusion detection system sing machine learning. IEEE 13th Annual Computing and Communication Workshop Conference (CCWC), Las Vegas, NV, USA, Pp. 0886-0892, doi:10.1009/ccwc57344.2023.10099340.

Alkanjr B. and Mahgoub A. I. (2023). A novel deception-based scheme to secure the location information for IoBT entities. IEEE Access. doi:10.1109/access.2023.3244138.

Askar S., Mustafa C. and Kareem S. (2021). Deep learning in IoT systems: A review. DOI:
10.5281/zonodo.5221646.

Bagaa M. Jorge B., B., and Antonio S. (2020). A Machine Learning Security Framework for
IoT Systems. Journal of IEEE Access. Vol. 8 pp 114069.

Bout E., Valeria L., Antoine G. (2021). How Machine Learning changes the nature of Cyber attacks on IoT networks: A survey. Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers.

Cameron L. (2021). Internet of Things Meets the Military and Battlefield: Connecting Gear
and Biometric Wearables for an IoMT and IoBT, IEEE Computer Society.

Cvitic I., Perakovic D., Perisa M. and Gupta B. (2021). Ensemble machine learning approach for classification in smart home. International Journal of machine learning and cybernetics. doi: 10.1007/s13042-020-01241-0.

Dehghantanha A., Azmoodeh D. A. and Choo K. K. R (2019). Robust malware detection for
IoBT devices using deep Eigenspace learning. IEEE transaction and sustainable computing 4(1), pp. 88-95. doi: 10.1109/tsusc.2018.2809665.

Denise E., Zheng W., A. Carter (2015). Leveraging the Internet of Things for a More
Efficient and Effective Military, A Report of the CSIS Strategic Technologies Program. Publication of Center for Strategic & International Studies, Washington, DC, USA.

DOI: 10.64290/bimagombe.v9i2A.1149

Elsayed M. S., Le-Khac N. A., Jahromi H. Z. and Jurcut A. D. (2021). A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs. 16th International Conference on Availability, Reliability and Security (ARES 2021), Vienna, Austria. doi.org/10.1145/3465481.3469190

Farooq M. J. and Zhu Q. (2017). Secure and reconfigurable network design for critical information dissemination in the Internet of Battle Things. Arxiv.1703.01224v1[cs.NI].

Fraga-Lamas P., Fernandez-Carames T. M., Manuel S. A, Castelo L. and Miguel G I. C. (2016). A review of IoT for defence and public safety. Sensors.16,1644, doi 10.3390/s16101644.

Francesco R, Salvatore D., and Tommaso M. (2018). Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking, IEEE Internet of Things journal, 1(1).

Galán, J.J.; Carrasco, R.A., LaTorre, A. Military Applications of Machine Learning (2022). A Bibliometric Perspective. Mathematics, 10, 1397. doi.org/10.3390/ math10091397

GlobalData (2019). Internet of Military Things, www.Globaldata.com.

Gotorane V. and Raskar S. (2019). IoT practices in Military applications. Conference paper. doi: 10.1109/ICOEI.2019.8862559.

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and Challenges in Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019, 1-14.

Hung, M., Gartner (2018). Leading the IoT: Gartner Insights on How to Lead in a Connected World, https://www.gartner.com/imagesrv/books/iot /iotEbook_digital.pdf

Hussain F., Rasheed H., Syed A. H. and Ekram H. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges, IEEE Communications Surveys & Tutorials.

Ibor A. E. 1, Florence A. O., Olusoji B. Okunoye and Obeten O. Ekabua1(2020). Conceptualization of Cyberattack prediction with deep learning. Springer Open Access publication. https://doi.org/10.1186/s42400-020-00053-7

IEEE Internet Initiative (2015). Towards the definition of the Internet of Things (IoT), https://iot.ieee.org/images/files/pdf/

Kang, J. J., Yang, W., Dermody, G., Ghasemian, M., Adibi, S., & Haskell-Dowland, P. (2020). No soldiers left behind: An IoT-based low-power military mobile health system design. *IEEE access*, *8*, 201498-201515.

Katalin E. B. (2018). Possibilities and Security Challenges of using IoT for Military Purposes. ORCID: 0000-0002-3697-7871

Kebande V. R. Nickson M. K. Richard A. I. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments, International. journal. Information Technology. 13(1):5–17. Springer publication.

Kott A., Swami A. and West B. J. (2016). The Internet of Battle Things. IEEE 49(12), 70-75.

Kudelsky Security (2018). IoT security reference architecture. A white Paper.

Kumar S., Prayag T., and Mikhail Z. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review, journal of Big Data, publication of Springer Open Access, doi.org/10.1186/s40537-019-0268-2.

Langleite R. S.,Griwodz C. and Frank T. Johnsen (2021). Military Applications of Internet of Things: Operational Concerns Explored in Context of a Prototype Wearable. International Command and Control Research and Technology Symposium (ICCRTS) Proceedings 2021.

Mancini F. and Johnsen F. T. (2021). A novel IoBT security assessment framework: LoRaWAN case study. Norwegian Defence Research Establishment. Paper ID 2.

Mbunge, E., Akinnuwesi, B., Fashoto, S. G., Metfula, A. S., &Mashwama, P. (2021). A critical review of emerging technologies for tackling COVID-19 pandemic. Human behavior and emerging technologies, 3(1), 25-39.

Meneghello, M. Calore, D. Zucchetto, M. Poleseand A. Zanella (2019). IoT:Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. IEEE Journal of Internet of Things, 6(5), pp. 8182-8201.

Neto. E.C.P., Dadkhah S., Ferreira R., Zohourian A., Lu R. and Ghorbani A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors, 23,5941, doi: 10.3390/s23135941.

Pal S., Hitchen M., Rabehaja T., Subhas M., (2020). Security Requirement for the Internet of things. A systematic approach. Sensors, 20(20), 5897.

Pham T. (2018). U.S. Army Research, Development and Engineering Command, AI & ML in Multi Domain Operations; NATO SET-262 Specialists' Meeting on *AI* for Military MultisensorFusion Engines Budapest, HUN, 5-6.

Prema R., Reddy K. K. and Lakshmi R. (2023). Robust malware detection for IoT devices using Deep Eigen Space Learning. An International of Creative Research Thought (IJCRT), 11(3).

Rachit, Shobha B. · Prakash R. R. (2021). Security trends in Internet of Things: a survey. SN Applied Sciences 3:121 | https://doi.org/10.1007/s42452-021-04156-9, Springer Nature Journal.

Radanliev P. David D. R. Rob W. · Max V. K. Rafael M. M. · La'Treall M. Omar S. Peter B., Eirini A. (2020). Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge, SN Applied Sciences 2:1773 | doi.org/10.1007/s42452-020-03559-4

Rajalakshmi K., Adarsh K, Dhanalekshmi G., Anand N. and Basit Q. (2020). An Overview of IoT Sensor Data Processing, Fusion, and Analysis Techniques, MDPI Publication, 20, 6076; doi:10.3390/s20216076.

Rutravigneshwaran P. and Aitha G. (2023). Security model of IoBT using trust and K-means Clustering Algorithm. IJCNA, 10(1). doi:10.22247/ijcna/2023/218514.

Said O. and Tolba (2021). A reliable and scalable Internet of Military Things architecture.

DOI: 10.64290/bimagombe.v9i2A.1149

Computers, Materials & Continua, 67(3), 3887-3906. doi: 10.32604/cmc.2021.016076

Sarker I H., Kayes A. S. M, Shahriar B., Hamed A., Paul W. and Alex N. (2020). Cybersecurity data science: an overview from machine learning perspective, Journal of Big Data, A Springer Open publication.

Sarker I. H., Furhad M.H., Nowrozy R. (2021). AI-Driven Cyber Security. An overview, security Intelligence Modelling and Research. SN computer Science 2(173). doi: 10.1007/542979.02100557-0

Sharma P., Najjar L. and Srinivasan S. (2023). Practical applications to prevent cyber-attacks in IoBT. Journal of Science and Information Technology. Pp17-24, doi: 10.5121/csit.2023.130602

Tawalbeh L. Fadi M., Mais T and Muhannad Q. (2020). IoT Privacy and Security: Challenges and Solutions. MDPI journal of Applied Science. 10:410. doi:10.3390/app10124102.

Syed N.F., Baid Z., Ibrahim A. and Valli C. (2020). Denial of Service attack detection through machine Learning for the IoT. Journal of Information and Telecommunication, 4.4,482-503, doi: 10.1080/24751839.2020.1767484.

Tortonesi M., Morello A., Govoni M., Michaelis J., Stefanelli C. and Russell S. (2020). Leveraging IoT within the military network environment- Challenges and Solutions.

Urla P. A, Mohan G, Tyagi S, Pai SN (2019). A novel approach for security of data in IoT environment. In: Computing and network sustainability. Springer, pp 251–259

Ullah, H., Nair, N. G., Moore, A., Nugent, C., Muschamp, P., & Cuevas, M. (2019). 5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases. IEEE Access, 7, 37251-37268.

Uday S. S., Andreas S. Cihan T. and Mike S. (2017). A brief survey of machine learning and their sensors and IoT applications.

Yang Y. (2018). Research on Military Application of IoT. International Conference on Education, Management and Information Technology

Zhu J., Egan Mc, Quan P., Sujay P., Sam R., Ryan S., and Andrew T. (2018). A Vision toward an Internet of Battlefield Things (IoBT): Autonomous Classifying Sensor Network. Journal of US Army Research Laboratory. Pp 1-27.