RESEARCH ARTICLE

Title: Security Trends in Internet-of-Things for Ambient Assistive Living: A Review

Ankit D. Patel[1], Rutvij H. Jhaveri*[2], Kaushal A. Shah[3], Ashish D. Patel[4], Rajkumar Singh Rathore[5], Manish Paliwal[6], Kumar Abhishek[7] and Dhavalkumar Thakker[8]

[1,2,3,6] CSE Department, School of Technology, Pandit Deendayal Energy University, Gandhinagar, India
[4] CSE Department, SVM Institute of Technology, Bharuch, India
[5] Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom
[7] Department of CSE, National Institute of Technology, Patna, India
[8] School of Computer Science, University of Hull, United Kingdom

ARTICLE HISTORY

Received:
Revised:
Accepted:

DOI:

Abstract: The Internet of Things (IoT) has revolutionized our society and become indispensable to modern existence. The IoT allows users to access their electronic gadgets from any location. The widespread adoption of IoT across sectors, from manufacturing to surveillance to elder care, has contributed to its rising profile. New security risks and challenges arise with the growth of the IoT. With the development of IoT, the likelihood of an attack by hackers has increased. The burden of addressing these dangers falls on researchers and security professionals. This article looks into the challenges of IoT security in a real-world Ambient Assisted Living (AAL) environment. This work discusses the numerous security attacks employed by cybercriminals in AAL IoT. In addition, this research investigates the varied responses to the risks. We discussed the state-of-the-art technologies available for protecting AAL IoT networks. This work analyses and compares the majority of the latest technologies available. In conclusion, we offer a few suggestions for where the field could go from the current scenario.

Keywords: IoT, Ambient Intelligence, Assisted Living, SDN, Fog Computing, Edge Computing, Blockchain, Artificial Intelligence.

1. INTRODUCTION

The Internet has become a necessity in everyone’s life nowadays. Spending even a day without the Internet makes a person frustrated. The reason is that almost all the devices that we use nowadays are connected to the Internet [1]. Electronic devices and gadgets like smartphones, tablets, smartwatches, and laptops have become an essential and inevitable part of human life. The interconnection of such devices and objects that we use in day-to-day life with the Internet gives rise to a domain that is popularly known as the “Internet of Things (IoT)” [2]. IoT comprises an extensive network that includes various devices, such as sensors which collect the data and pass it on to the other devices where the data is processed and a task is performed based on the data [3] [4]. IoT devices can be connected through wired or wireless mediums. IoT is also the network interconnecting dynamic and self-configuring devices for communicating data using existing technologies [5]. Over the past few years, IoT devices have become very popular across the globe. By 2025, it is estimated that around 75 billion IoT devices will be operating through the Internet worldwide [6]. IoT devices are self-configured and can operate without human intervention, transforming traditional devices into smart devices. [4]. The IoT has transformed real-time objects into intelligent machines. [7] [8]. IoT reduces human interaction in many scenarios by introducing automation in systems and enabling machine-to-machine (M2M) communication [9]. In simple terms, IoT can be understood as providing “anytime, anywhere, and anything” access to the system [10].

The growing popularity and acceptance of IoT technology bring forth various security challenges [11]. The nature of IoT devices and the operation of the network make the IoT susceptible to multiple threats [12]. The majority of security issues arise in IoT networks due to a lack of awareness about security and the deployment of weak security mechanisms, such as the use of weak passwords or failure to change passwords, as well as the use of insecure channels, among other factors [13] [14]. The small size of IoT devices and their limited resources further complicate the implementation of robust security mechanisms on these devices [15].

Security in the IoT for assisted living facilities has recently garnered the attention of many researchers. As depicted in Figure 1, a significant portion of IoT devices in assisted living (AAL) require careful attention to ensure safe data transmission for the effective functioning of the entire AAL ecosystem. Several methods have been proposed by researchers to ensure the security of AAL IoT devices. This research examines the state-of-the-art techniques currently employed to safeguard AAL IoT systems. The review categorizes various approaches to implementing security in AAL and provides a comparative assessment of these methods with previously published studies in the field. Furthermore, the paper includes information on the security features provided by each solution and the respective simulator or emulator used, which is often omitted in existing reviews. The paper follows the following structure: Section 2 presents two related surveys, while Section 3 provides the history of the IoT. The classification of IoT security threats is presented in Section 4, and Section 5 discusses the various security measures available for protecting IoT systems. Section 6 offers a discussion and suggestions for future research, and Section 7 provides a summary and concluding thoughts.

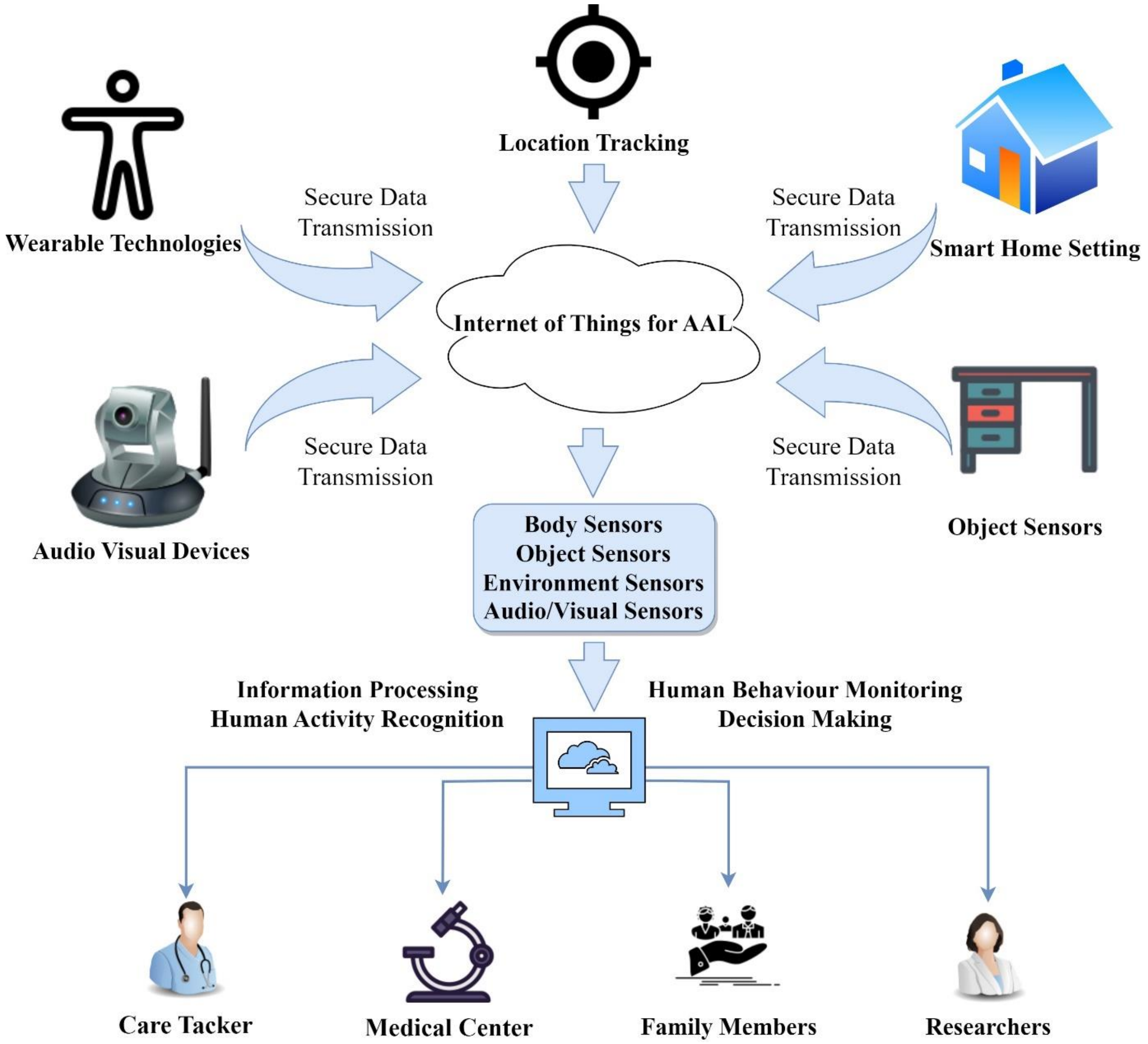

Figure 1: Security concerns in IoT for ambient assisted living environment

2. RELATED SURVEYS AND CONTRIBUTIONS

Many researchers have significantly contributed towards securing IoT systems for AAL applications. This section presents a comparative analysis of various review articles proposed by different researchers.

In [16], the authors present a state-of-the-art survey of various security mechanisms for securing healthcare systems. The paper discusses the security and privacy issues in Healthcare 4.0 and provides a review of different solutions employed for healthcare security. Rachit et. al. in [17] present an overview of the security challenges in IoT protocols and standards. It provides a classification of the attacks in IoT and offers a brief comparison of different categories of solutions for IoT security. This survey primarily focuses on security in protocol-based attacks and data-based attacks. The authors in [18] discuss secure transmission techniques in IoT for AAL systems, including cluster-based models, location-based models, Blockchain-based models, and trust-based models. The researchers survey recent mechanisms, which encompass cryptography solutions and energy-efficient solutions. In [19], the authors provide a review of cryptography techniques for securing IoT networks. They present a systematic review of various encryption approaches, such as private key encryption, public key encryption, and hybrid approaches. The paper compares different algorithms based on security services like confidentiality, integrity, and more. Additionally, the study explores various attacks on encryption approaches, along with state-of-the-art techniques to mitigate their impacts. The review of authentication techniques is presented in [20]. The authors present a taxonomy of security attacks that hinder authentication in IoT. The paper surveys methods for mitigating authentication attacks, including password-based methods, token-based methods, biometric authentication methods, cryptography approaches, and multi-factor authentication methods. The authors conduct a comparative analysis of these techniques based on evaluation parameters like packet delivery ratio, communication cost, storage cost, end-to-end delay, memory consumption, and more.

In [21], Soo et. al. present a survey of security measures in industrial applications of IoT. The authors examine security mechanisms based on the CIA (Confidentiality, Integrity, and Authentication) requirements. The paper identifies issues at each layer of the IoT architecture and presents security mechanisms to address these issues in industrial IoT. It specifically focuses on IP-Sec, cryptography, and hash function mechanisms as countermeasures to attacks in industrial IoT. In [22], the authors present a detailed taxonomy of security attacks in IoT and propose a set of security mechanisms to counteract them. The paper also provides an analysis of machine learning solutions for IoT security, specifically focusing on supervised and unsupervised learning approaches. It also highlights the research challenges faced in applying machine learning techniques for securing IoT. The authors in [23] list various security threats at each layer of the IoT architectural model. The paper presents security issues based on different applications and surveys of classical security mechanisms like encryption, as well as advanced security techniques like SDN and blockchain. Furthermore, the paper includes a comparative analysis of encryption, SDN, and blockchain techniques, and provides research directions for future exploration. Parushi et al. in [24] present a taxonomy of IoT attacks, vulnerabilities, and anomalies in IoT networks. The authors focus on Intrusion Detection Systems (IDS) using learning algorithms to detect anomalies in networks. The paper explores various types of learning solutions for security in IDS, such as supervised learning, unsupervised learning, reinforcement learning, federated learning, deep learning, and more. It also includes case studies that demonstrate the application of learning techniques in IoT scenarios. In [25], the authors discuss various security issues and attacks in IoT, with a specific focus on authentication techniques. The paper presents a comparative analysis of different authentication mechanisms, including ID-based authentication, ECC-based authentication, certificate-based authentication, and blockchain-based authentication.

In [26], Sohel et al. discuss network vulnerabilities and resource management in IoT. The paper compares different backdoor detection mechanisms, such as Special Credentials, Hidden Functionality, and Unintended Network Activity, in IoT. The authors present the challenges faced in implementing backdoor solutions and propose research ideas for future exploration. The authors in [27] address security issues at different layers of the IoT architecture, focusing on detecting Distributed Denial of Service (DDoS) attacks in IoT networks. The paper reviews intrusion detection systems that employ anomaly detection techniques using machine learning and deep learning. Additionally, the authors discuss challenges associated with the proposed solutions and provide potential solutions to overcome them. Mohit et al. in [28] present the security challenges in IoT from a user's perspective. The paper reviews biometric-based authentication techniques to secure IoT applications from unknown users. It compares physical-based biometric authentication systems with behavioral authentication schemes and explores various behavioral schemes that utilize machine learning techniques for user authentication. The authors in [29] present a taxonomy of attacks at different layers of the IoT architecture. The paper reviews solutions in various categories, including machine learning, deep learning, and cryptography, Blockchain, and anomaly detection in intrusion detection systems (IDS), to mitigate attacks in IoT. The authors also discuss the challenges associated with implementing these solutions. In [30], the authors highlight the security enhancements achieved by Software-Defined Networking (SDN) in IoT. The paper also discusses the challenges that SDN introduces to IoT networks. Additionally, the authors review machine learning solutions that add intelligence to SDN controllers to address the challenges of SDN in IoT networks.

The authors in [31] discuss security and privacy issues in IoT. The paper reviews solutions related to intrusion detection systems and trust mechanisms to address privacy concerns in IoT. It also presents open research challenges in existing security and privacy solutions. In [32], the authors classify security attacks in IoT and address security issues prevalent in IoT technology. The paper reviews solutions in cryptography, blockchain, trust models, and SDN-based approaches to mitigate the impact of threats in various IoT applications. The authors in [33] discuss state-of-the-art security issues and challenges in IoT. The paper studies the impact of security threats in different IoT applications and reviews trust management, authentication, privacy, encryption, and fault tolerance techniques. The authors also present the latest challenges in IoT security and propose future research directions. In [34], the authors provide a comprehensive review of privacy and application layer issues in IoT. The paper reviews approaches that address challenges faced by conventional techniques such as encryption schemes, key management, and authentication methods like token-based and context-based authentication. The authors also discuss homomorphic cryptography solutions for authentication in IoT. In [35], the authors focus on security issues with lightweight, resource-friendly solutions. The paper reviews solutions for achieving authentication and integrity security features in IoT and provides a security analysis of lightweight integrity and authentication schemes. Lastly, the authors identify research gaps for future exploration. The authors in [36] present a review of trust-based approaches for securing IoT networks. The paper includes a comparative analysis of the performance of various trust models under different attacks. The authors also discuss research challenges related to deploying trust models in intrusion detection systems.

Most of the surveys discussed above provide an analysis of the issues and challenges involved in securing IoT networks. The surveys mentioned above primarily focus on specific categories of solutions such as encryption, machine learning, and others. However, they often lack the inclusion of implementation details such as the specific simulators or emulators used to implement these solutions. Table I presents the summary and contributions of the existing surveys and our survey. In contrast to the aforementioned surveys, our survey provides a comprehensive description of various categories for securing IoT networks. These categories include Fog Computing, Edge Computing, Software-Defined Networking (SDN), Blockchain, Machine Learning (ML), and Lightweight Cryptography. Additionally, our survey goes beyond the issues and challenges by including implementation details, such as the specific tools or frameworks utilized in the implementation of these approaches. This aspect enhances the practicality and applicability of our survey in the field of IoT security.

TABLE I: COMPARISON OF RELATED SURVEYS

Surveys	IoT Architecture	IoT Applications	Security Issues	Security Requirements	Attacks in IoT	Lightweight Cryptography Solutions	Fog Computing Solutions	Edge Computing Solutions	SDN solutions	Blockchain Solutions	Machine Learning Solutions	Discussion	Future Directions
[16]	Yes	Yes	Yes	Yes	No	Yes	No	No	No	Yes	Yes	Yes	Yes
[17]	Yes	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	No
[18]	Yes	No	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes	No
[19]	Yes	No	Yes	Yes	No	Yes	No	No	No	No	No	Yes	No
[20]	No	No	No	No	Yes	Yes	No	No	No	Yes	No	Yes	Yes
[21]	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	No
[22]	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes
[23]	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes
[24]	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes
[25]	Yes	No	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No	No
[26]	Yes	No	Yes	Yes	Yes	No	No	No	No	No	No	Yes	Yes
[27]	No	No	Yes	Yes	No	No	No	No	No	No	Yes	Yes	Yes
[28]	No	No	Yes	No	No	No	No	No	No	No	Yes	No	Yes
[29]	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes
[30]	No	No	Yes	No	Yes	No	No	No	Yes	No	Yes	Yes	Yes
[31]	No	No	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes
[32]	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	Yes
[33]	No	No	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes
[34]	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No

[35]	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes
[36]	No	No	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Our Survey	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

3. STATE OF THE ART

To identify the challenges in the security area of Ambient Assisted environments using the IoT, a systematic literature review was conducted over the past 10 years. The review process involved gathering data from various sources, including online databases, offline resources, and library materials. In the first stage, relevant literature was collected using search terms such as security, IoT, Ambient Intelligence (AI), SDN, fog computing, ML, and deep learning (DL) for AAL in IoT. Multiple online platforms and databases were explored, including the ACM digital library, CiteSeerX, Compendex, DBLP computer science bibliography, Index Copernicus, arXiv, the Indian Citation Index (ICI), Inspec, Mendeley, Microsoft Academic, the Scientific Information Database (SID), Ulrich's Periodicals Directory, Google Scholar, as well as renowned publishers such as IEEE, Springer, and Elsevier. Additionally, Ph.D. theses from different universities were also consulted. In the second stage, each research article was evaluated based on its reference list, citation count, and ranking. This allowed for the inclusion or exclusion of articles based on their relevance and significance to the study. By following this rigorous methodology, the review was able to identify and analyze the challenges in the security domain of Ambient Assisted environments using the IoT, providing valuable insights into this field.

A. Overview of Ambient Assisted Living

The population of elderly individuals has experienced significant growth in recent years, thanks to advancements in medical facilities [37]. Along with the medical challenges that come with aging, elderly people also face various non-medical issues, including social isolation and loneliness. To address these challenges, Ambient Assisted Living (AAL) has emerged as a solution that leverages technology to improve the lives of the elderly.

The primary objective of an AAL system is to enable independent living for the elderly and enhance their confidence in performing daily activities, which may have become difficult with age [38]. By incorporating IoT technologies, AAL systems have become a promising and innovative technological solution for elderly care [39]. These systems offer various benefits to elderly individuals, helping them overcome social barriers, stay connected, and maintain a sense of independence.

B. IoT Architecture for AAL systems

It is indeed true that there is currently no standardized architecture model for Ambient Assisted Living (AAL) systems. Various researchers and research organizations have developed different IoT architectural frameworks to cater to the specific requirements of AAL applications. However, a common and fundamental model for IoT frameworks in AAL systems typically includes three layers: the sensing layer, network layer, and application layer as shown in below Figure 2.

1) Sensing Layer/Perception Layer:
   The Sensing layer in the IoT framework for AAL systems is also referred to as the perception layer or the physical layer in some literature. Its main purpose is to gather information about elderly individuals by using sensing devices. The Sensing layer is comprised of physical devices such as RFID tags, sensors, and actuators. These devices are responsible for sensing or collecting data from the environment or the individuals themselves. For example, sensors can be used to monitor vital signs, activity levels, environmental conditions, and other relevant parameters. RFID tags may be employed for tracking objects or individuals within the AAL environment [42]. Various types of sensors are available to meet specific requirements, including temperature sensors, infrared sensors, gyroscope sensors, accelerometer sensors, soil moisture detection sensors, and others [4]. These sensors collect data about elderly people and their environment. To establish connectivity between various devices, including sensors and actuators, gateway

nodes are utilized. This connectivity is facilitated through different communication protocols and networks such as local area networks (LAN), Bluetooth, ZigBee, Personal Area Networks (PAN), and wide area networks. Wide area networks can support technologies like LTE (Long-Term Evolution), GSM (Global System for Mobile Communications), GPRS (General Packet Radio Service), and others [42]. Once the data is collected, it is forwarded to the upper layers of the IoT architecture for further processing and analysis.

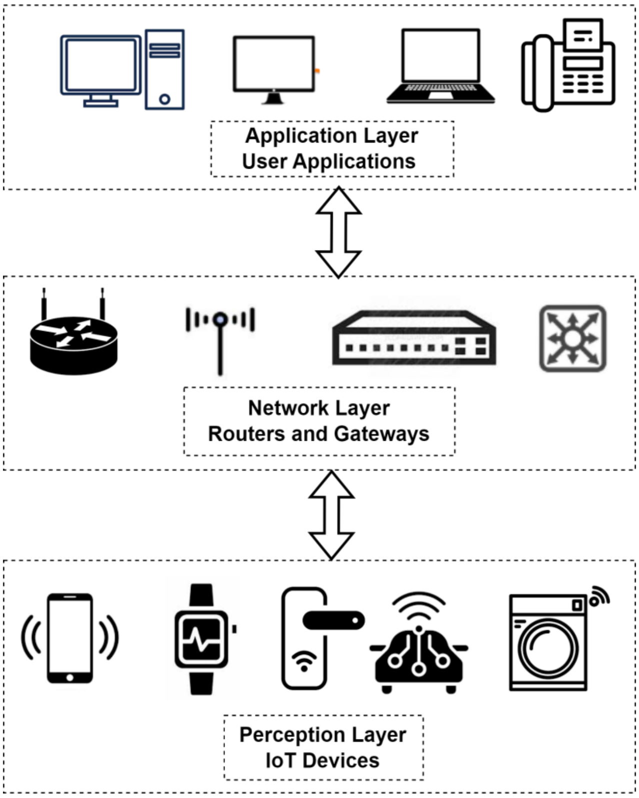

Figure 2: IoT layered framework architecture

2) Network Layer:
The network layer plays a crucial role in the architectural framework. Its main function is to manage and process the data obtained from the sensing layer. The network layer handles tasks such as data routing, data aggregation, and data transmission between different components of the system. [41]. The network layer in the AAL system is responsible for addressing the nodes and uniquely identifying them within the network [43]. The heterogeneous data gathered by the sensing layer is taken care of by the network layer [44]. The network layer in the IoT framework architecture also takes care of routing mechanisms to allow the transmission of data between the source and destination [45]. Some technologies operating at the network layer include 6LoWPAN, a low-power personal area network following the IPv6 addressing scheme, a routing protocol for low-power and lossy networks (RPL), and others. [42] [45].

3) Application Layer:
The application layer's task is to facilitate user access to the system by presenting processed data to the user and forwarding user-generated data to the lower layers. [45]. The application layer is also responsible for providing a user-friendly interface that is easy for elderly people and their caregivers to adapt to the technology. It may offer a web interface through which users can communicate with low-level devices. The key protocols operating at this layer include the Constrained Application Protocol (CoAP), which enables data transfer over the web using a request-response mechanism between network nodes, the Message Queuing Telemetry Transport (MQTT) protocol for lightweight message communication, the Extensible Messaging and Presence (XMPP) protocol that supports messaging applications, and the Advanced

Message Queuing Protocol (AMQP) used for exchanging business messages between organizations [42][45][46].

C. Applications of AAL Systems

Ambient Assisted Living (AAL) has brought about a revolutionary change in the daily lives of elderly people and their caregivers. Through the use of compact-sized sensors, enhanced processing capabilities, and the ability to handle diverse and heterogeneous data, AAL has found its application in almost every aspect of our daily lives. [4]. AAL applications span various domains, encompassing home applications, the healthcare sector, environment monitoring, smart cities, and many others [47].

1) Smart Cities:
   IoT technologies are employed in urban transport systems to facilitate vehicle-to-vehicle communication [48]. The AAL systems help elderly people safely commute from one place to another. The AAL systems offer other services like traffic management, pollution monitoring and control, smart parking systems, and many more. [49]

2) Healthcare:
   AAL systems have a significant impact on the medical and healthcare sectors by offering various services such as monitoring vital parameters, reporting emergencies, and providing medical recommendations. [7].. The sensors collect the person's health readings, such as blood pressure and heart rate, among others. The collected data is then analyzed, and IoT devices perform reactive diagnostic actions based on the analysis. Devices like heart rate monitors, blood pressure monitors, oxygen level monitors, and others are equipped with IoT sensors and actuators for this purpose.

3) Smart Home:
   The majority of elderly people prefer to stay in their homes due to various barriers and limitations they may face [50]. The home can be transformed into a smart home by incorporating electronic equipment and sensors, which automate daily tasks without requiring human intervention [7]. IoT devices are integrated into various home appliances such as lights, air conditioners, security systems, and CCTV cameras. These devices operate based on sensed conditions provided by the sensors, allowing elderly people to perform various tasks such as cooking and activities of daily living more efficiently and conveniently.

4) Wearable Devices:
   Wearable devices have become very popular in recent years due to their compact size. Varieties of bands are used to measure the physical activities of elderly people and are equipped with a GPS to track their location. These bands are equipped with sensors to record the data and software to analyze this data and provide measures or recommendations in reaction to the sensed data of the user.

5) Environment Monitoring:
   The AAL systems are used for monitoring the environmental parameters to provide a pleasant environment to elderly people. The sensors are deployed to sense the levels of the harmful substances in the environment like the emission of toxic gases [42]. The AAL systems are also used in Weather monitoring, Water monitoring, etc.

6) Independent Living:
   IoT technology has significantly benefited elderly and dependent people in their daily activities. With the help of IoT devices, elderly individuals can monitor their health without relying on external assistance. IoT applications in elderly care encompass various solutions such as fall detection systems, safety solutions, and tele-assisted solutions, which contribute to improving the quality of life for the elderly and dependent individuals. These advancements in IoT technology have made it easier for aged and dependent individuals to live more independently and safely.

D. Issues and Challenges in IoT for AAL Systems

The IoT has indeed revolutionized numerous domains of life and business worldwide. Its widespread adoption has brought significant benefits to many people. However, along with these benefits, the IoT also presents various risks and challenges. Researchers have extensively studied and identified the challenges that the IoT faces in its applications. In this section, we provide a summary of these issues and challenges to provide a comprehensive understanding of the hurdles that need to be addressed to maximize the potential of IoT technology.

1) Availability: Availability refers to ensuring that both hardware and software services are accessible to users, even in the event of device or network component failures [9] [51]. The limited availability of IoT services in time-critical applications can result in significant losses for AAL applications. To mitigate this issue, the concept of redundancy is employed to enhance availability to some extent [10].

2) Scalability: Scalability in the context of AAL systems refers to the ability to add new devices without disrupting the normal operations of the existing infrastructure [11]. As the elderly population continues to grow rapidly, the number of devices used in AAL systems also increases. Incorporating new devices while ensuring the smooth functioning of existing ones is a crucial task. The addition of new devices may require support for different protocols and standards, which poses a challenge in terms of integration and compatibility with the current application [9].

3) Lack of Standardized Architecture: The absence of a universally accepted architecture model for IoT in AAL systems presents a challenge. As the number of devices and communication technologies used in AAL applications continues to grow, there is a need for a standard architecture model that can serve as a foundation for building any AAL application. Such a model would provide consistency, interoperability, and ease of integration across different AAL systems, enabling seamless communication and interaction among devices and applications [9] [51] [52].

4) Heterogeneity: The integration of devices with different architectures and data formats in an AAL system presents numerous operational challenges. Each device may have its own unique architecture, communication protocols, and data formats, making it difficult to establish seamless interoperability and data exchange between them. Failure to overcome these integration challenges can result in data inconsistencies, communication failures, and limited functionality of the overall AAL system. [53].

5) Resource Constraints: The resource limitations of IoT devices, such as low memory and limited battery backup, present significant challenges in AAL systems. These constraints impact the performance and functionality of the devices, especially when dealing with complex algorithms or processing large volumes of data. The limited processing power of IoT devices can lead to slower data processing and reduced computational capabilities, affecting the real-time responsiveness and overall efficiency of the AAL system [54].To address these challenges low-weight algorithms need to be designed for the resource constraint devices.

6) Reliability: Data communication in AAL systems occurs via the Internet or other public domain networks. However, this transfer of data through public channels can potentially result in data alteration or destruction [4]. Thus, communication needs to be facilitated by the error detection and correction mechanism to ensure reliable data transfer.

7) Security: AAL systems are vulnerable to numerous security threats due to their inherent characteristics. Easy access to nodes within the AAL system poses a risk to data security. Therefore, it is crucial to implement robust authentication and privacy mechanisms before transmitting data over shared mediums [55].

8) Intelligence: The majority of the AAL systems are considered smart systems where the system acts according to a set of predefined rules [56]. The AAL systems would be better if the system could incorporate the behavioral and situational changes of elderly people, which can be incorporated through learning and adaptive mechanisms.

9) Identification: The number of IoT devices in the AAL systems is increasing swiftly. This increase in the number of devices results in the issue of assigning the IP addresses to the devices. The IPv4 address space would not fit the devices, and thus, the Ipv6 addressing scheme needs to be applied. The application of the IPV6 addressing scheme would increase the efforts of the network administrator in re-configuring the devices in the AAL systems.

4. SECURITY CHALLENGES AND REQUIREMENTS IN AAL SYSTEMS

A. Security Issues in AAL systems

The AAL domain has gained wide popularity due to its assistive solutions for elderly people. However, along with its benefits, there are also various security threats and vulnerabilities that need to be addressed. One of the reasons for these security breaches in AAL systems is the heterogeneity present within the systems [57]. The inconsistencies in architectures and standards among devices in AAL systems lead to various challenges and difficulties in maintaining consistent security mechanisms. The heterogeneity of data, stemming from the differences in devices, poses additional obstacles to effective security measures. [58]. Resource constraints on IoT devices, including limited processing power, memory, and energy, pose significant challenges to ensuring robust security. The limitations of these low-capacity devices make them more susceptible to security vulnerabilities. Traditional security mechanisms may not be suitable or effective in IoT devices due to their resource constraints. Innovative approaches and lightweight security protocols are required to address security concerns in IoT environments.

With the exponential growth of devices in AAL systems, there is a corresponding increase in the volume and variety of data generated. This large volume of data presents security challenges, including the potential for malware injection and resource consumption [59]. Due to the widespread popularity of AAL systems and the desire to gain a competitive advantage, many vendors and manufacturers are often eager to release their devices quickly. Unfortunately, this sometimes leads to a lack of sufficient attention being paid to the security aspects of these devices. In their haste to bring products to market, security measures may be overlooked or not given the necessary priority [60].

The communication of the data in the AAL systems majorly happens through the public domain network namely the Internet. The data is transferred via insecure channels which lure the attackers to steal the data. The data needs to be secured from such attackers during the transmission. The Internet is open to all and hence the devices in the AAL systems are also vulnerable to various security threats. There is no common architecture for the AAL systems and hence no common security framework for the applications. The security policies differ from application to application which again creates a loophole in the system from the security point of view. The lack of security mechanisms like authentication mechanisms and encryption mechanisms also makes IoT systems vulnerable [13] [61].

B. Security Attacks in Ambient Assisted Living

The AAL systems are exposed to plenty of security threats and vulnerabilities. The AAL applications are susceptible to a variety of security attacks that tend to degrade or halt the performance of the system [62] [63]. Many attacks occur at different layers in the IoT architecture model, which are discussed in the below subsections.

1) Threats at Perception Layer/Sensing Layer:
The perception layer consists of physical components like the sensors and the actuators. The majority of the device vendors take less care about security considerations, and thus these devices operate in an open

environment where a large variety and high volume of data is transferred through unguided media which lures the attacker to attack the system [64]. Some of the major threats that occur at this layer include spoofing attacks, node capture attacks, eavesdropping, and RF Jamming [31].

In the node capture attack, the attacker tries to capture a node or replace one node with another node [65]. This replacement of the node may result in data loss at the nodes, accessing sensitive information, and many more. In the Eavesdropping attack, the attacker's motive is to intercept the data of the user. This type of attack occurs during data transmission through insecure channels [24]. In the RF Jamming attack, the attacker inserts the dummy radio signals often known as noise to disrupt the data signals which jam the RFID systems [66]. In Malicious Code Injection, the attacker tends to append the malicious code inside the normal data and send it to the legitimate node. The attacker's goal in this attack is to cause destruction to the node or carry out any undesirable activities by the node. In the Spoofing attack, the attacker aims to impersonate the legitimate nodes by claiming themselves as the legitimate nodes [31]. The attacker's goal is to make others believe that he is the legitimate node.

2) Threats at the Network Layer:

The network layer consists of the devices like routers and gateways; which are involved in the logical addressing of the nodes and the routing of the data. IoT is an interconnection of many networks which poses many security problems [29]. To disrupt the network activities, the attackers perform attacks which include Denial of Service, Man in Middle Attack, Sybil Attack, Blackhole attack, Grayhole attack, and Wormhole Attack.

In a Denial of Service attack (DoS), the attacker aims to disrupt the normal operations of the network by either flooding unnecessary data packets or by misbehaving during the routing activities [24]. The attacker attacks with the vision of making the network services unavailable to the users by launching the DoS attack [67]. In the Replay attack, the attacker forwards the same data packet again and again to the legitimate node to deplete the resources of the node [25]. The Sybil attack creates the multiple identities of a legitimate node and presents it to the network to present false information about the legitimate node [31]. In the Man in the Middle attack, the attacker tends to intercept the data intended for the receiver and sends fabricated data to the receiver by pretending to be the source node. Thus the receiver will believe that the data is sent by a legitimate source but in fact, it is by an attacker. The Blackhole attack tries to capture the network traffic by claiming that it has the shortest and the fresh route to the destination. The attacker in this attack intercepts the data packets and drops them and does not forward those [68]. The Grayhole attack is the enhancement of the blackhole attack [69]. In this attack, the attacker claims to have the shortest path to the destination through routing misbehavior like the blackhole attack. After being part of the route, the attacker forwards some data packets and drops some of the packets [70] [71]. In a Wormhole attack, the attacker intercepts the packets at one location and then tunnels them through different locations [72].

3) Threats at the Application Layer:

The application layer is in charge of providing the interface for accessing the system to the users. The direct interaction of this layer with the user brings many security threats and vulnerabilities [27]. Some of the attacks are the application layer are viruses, worms, Trojans, phishing attacks, and sniffing attacks [27] [31]. In a Sniffing attack, the attacker monitors the user activities through sniffing tools and intercepts the data. The objective of the sniffing attack is to intercept the user's data through monitoring. Viruses and worms are malicious programs that are injected into the systems by the attacker to force the device to perform undesired activities. The Phishing attack sends the fraudulent luring offers and data to the legitimate nodes and creates an impression that the data has been sent by a normal node [73]. The summary of various attacks is discussed in Table II.

Table II: Summary of different attacks in IoT

Layer	**Attack**	**Description**	**Possible Remedies**
Perception Layer	Node Capture Attack	Hijacking a node or replacing the legitimate node with the attacker node	authentication mechanisms
Perception Layer	Eavesdropping	Intercepting the data in transmission occurring through insecure channels	Encryption techniques
Perception	RF Jamming Attack	Adding the Radio Signals to the data signals of the same	Checksum, Hash

Layer		frequency distorts the data	algorithms
Perception Layer	Spoofing Attack	Impersonate the legitimate node and claim to be a legal node	Authentication mechanisms
Perception Layer	Malicious code Injection	Injecting the malicious code to force the legitimate node to perform undesirable activities	Data Inspection, Intrusion Detection Systems
Network Layer	Denial of Service Attack	Prevent the users from accessing the services in the networks	Traffic Monitoring, Data Inspection
Network Layer	Replay Attack	Transmission of the same data multiple times to a node to deplete the resources of the node	Traffic Monitoring, Data Packet Inspection
Network Layer	Sybil Attack	Creating multiple identities of a node and presenting false information about the node to the network	Traffic Monitoring, Intrusion Detection Systems
Network Layer	Blackhole Attack	Claiming to have the fast route to the destination and intercepting the data destined for the destination node and dropping the packets	Control packets monitoring during routing, promiscuous mode monitoring
Network Layer	Grayhole Attack	Claiming to have the fast route to the destination and forward some data packets and drop some data Packet	Control packets monitoring during routing, promiscuous mode monitoring
Network Layer	Wormhole Attack	Intercept the data in transmission and tunnel the data through a different path	Intrusion Detection Systems, Path Monitoring
Application Layer	Sniffing Attack	Records the activities of the user through sniffing tools	Port Scanning
Application Layer	Virus and Worms	Activate the malicious programs on the node to force them to perform undesirable tasks	Firewalls, Used of secure channels for communication
Application Layer	Phishing Attack	Lure the legitimate nodes to disclose sensitive information through offers	Filtering of data, Firewalls
Application Layer	Trojans	Injecting the malicious code into normal data In the node to perform undesirable activities	Port Scanning, Firewalls, Use of secure channels

1. *Security Requirements in AAL systems*

The above sections describe various threats and attacks at different layers of the IoT architecture model for the AAL systems. Thus proper security mechanisms need to be designed for overcoming the negative impacts of such threats. The security solutions designed to overcome the effects of the attacks need to meet some of the security requirements which are discussed below.

1) Confidentiality: Confidentiality ensures that data is accessible only to authorized parties involved in communication, restricting access for all other entities. In the context of AAL systems, it is crucial to limit access to sensitive data about elderly people to legitimate parties. A solution claiming to achieve confidentiality provides a guarantee that the data, particularly sensitive information, is securely handled [74]. To ensure confidentiality, mechanisms like encryption and transposition functions can be used. As the encrypted data travels through the network, the attacker needs to decrypt the data to access it which can be done only by the communicating parties [25].
2) Integrity: Integrity ensures that the contents of data cannot be altered by unauthorized users. It guarantees the accurate delivery of data, ensuring that the receiver receives the exact information as sent by the sender. The primary objective of achieving integrity is to prevent unauthorized data modification [26]. Modification of data in the AAL system can cause severe damage to elderly people. To achieve Integrity, encryption approaches can be used and apart from cryptography techniques, Hash algorithms are also helpful to achieve Integrity [25]
3) Authentication: Authentication refers to verifying the identity of the users as they claim to be [75]. The device needs to first prove its identity and also needs to verify the identity of the receiving device [26]. The simplest way of achieving authentication is using passwords for the access of the devices. But with the advancement of technologies and intelligent mechanisms, the attackers are successful in cracking and stealing weak passwords [25]. Thus, advanced security mechanisms are needed to achieve authentication. Other forms of authentication mechanisms like biometric authentication, Smart cards, and RFID tags are also used.
4) Availability: Availability is a crucial security requirement in the AAL system. It ensures that the resources necessary for legitimate nodes are accessible at all times. The uninterrupted availability of the system is

essential to prevent potential hazards and ensure the well-being of elderly people. However, attackers may attempt to disrupt availability by launching various attacks, such as flooding to drain the battery life of nodes or denial of service attacks to restrict access to services. To achieve and maintain availability, techniques such as anomaly detection, intrusion detection systems, and traffic monitoring can be employed.

5) Non-Repudiation: Non-repudiation ensures that the communicating parties cannot deny their involvement in communication activities. Once data is sent by the sender or received by the receiver, they cannot later claim that they did not participate in the exchange. Non-repudiation prevents the denial of data exchanged between parties [72].
6) Authorization: The Authorization requirement deals with the rights and the privileges assigned to the users in the IoT system [25]. This requirement states that the user should access the resources which are their right to access and any unauthorized access should be avoided. The update or access of the data should also take place by authorized entities only.

5. SECURITY SOLUTIONS

As discussed in the previous section, AAL applications are deployed under numerous threats. To overcome the negative effects of these threats and attacks in AAL systems, researchers have designed various solutions. The following subsections describe some of the emerging technologies used to mitigate security attacks. This section discusses the various algorithms involved.

A. Lightweight Cryptography Solutions

Cryptography involves converting data into a format that is difficult for attackers to understand. The original data is referred to as plain text, while the converted data is known as cipher text. Encryption is the process of converting plain text to cipher text, and decryption is the process of converting cipher text back to plain text. These processes rely on algorithms and keys. Maintaining the secrecy of the key is crucial in cryptography. However, conventional cryptography algorithms may not work effectively in IoT devices due to the resource constraints in AAL systems [76]. As a result, algorithms that demand high processing power and storage are not practical for implementation on devices in AAL systems. Consequently, a new field known as lightweight cryptography has emerged. It encompasses cryptography approaches that require less computation power and storage space, making them suitable for deployment in resource-constrained devices within AAL systems [35] [77]. There are two basic approaches to cryptography, namely symmetric cryptography and asymmetric cryptography [78]. In symmetric cryptography, the same key is used for the process of encryption and decryption whereas in the case of asymmetric cryptography, different keys are used for encryption and decryption [79].

Chandi et. al. in [80], present a symmetric approach that utilizes the Data Encryption Standard (DES) algorithm for the encryption and decryption of IoT device data. The findings of the study demonstrate that the DES algorithm outperforms other conventional algorithms in terms of encryption and decryption speed. This approach provides confidentiality to the data. In [78] and [81], the authors demonstrate the utilization of the Advanced Encryption Standard (AES) algorithm to ensure the security of data generated by IoT devices. This approach ensures confidentiality and offers protection against side-channel attacks. AES is an enhanced version of the DES algorithm, featuring longer key lengths and more rounds in the encryption process. In [82], the authors explore the implementation of the AES algorithm in agricultural applications. Specifically, they focus on the use of remote control devices in farms for various activities. To ensure secure data transmission within agricultural land, AES encryption with a 128-bit key is employed. The results of the study demonstrate that this approach offers enhanced security and reliability compared to the use of the DES algorithm.

A substitution cipher technique based on the Fiestal structure is presented in [83]. This symmetric block cipher approach processes a block of 64 bits with a 64-bit key. The presented approach tends to provide confidentiality during data transfer. The results show this approach has less computational overhead, but key management becomes an issue in this symmetric algorithm. Wang et al. in [84] presented an asymmetric approach comprising dynamic curves in the ECC (Elliptic curve cryptography) algorithm in the Internet of- Vehicles (IoV). The data transmitted by the vehicles are stored as dynamic curves. The results show that the algorithm works fine with less computational time for small key sizes. A privacy-preserving approach is presented in [85], which tends to protect the data on unsecured channels. This approach makes use of the RC4 stream cipher algorithm along with the logistic mapping to deal with the resource constraints problems of the IoT devices. This approach has less computation time, but the keys' transfer needs to be handled securely.

A lightweight authentication scheme has been presented in [86] for wearable devices. This algorithm employs the use of the XOR and the one-way cryptography hash functions for the authentication of devices sending the data. The XOR and the simple hash functions are designed for the resource constraint devices. Another lightweight authentication scheme is proposed in [87] which employs the use of the hash function for the mutual key agreement and key exchange in the wireless sensor networks. This approach employs a signature-based scheme where the node among a group is selected as the middle node, and this node handles the signature generation and verification process. Sliman et. al. in [88] presented a lightweight block cipher technique named the Ultra-Lightweight method which comprises three different methods namely bit-slice, and WTS. This approach is efficient in terms of computation time, diffusion, and confusion levels.

In [89], the authors demonstrate a lightweight device-to-device cryptography system that tends to achieve authentication, confidentiality, and integrity of data in the IoT network. This approach makes use of ECC cryptography and Authenticated Encryption Associated Data (AEAD) ciphers which provide security against many attacks like eavesdropping, impersonation, and spoofing attacks This approach is efficient in terms of providing security but has high computation time. In [90], the authors presented an optimized ECC-based approach named CooPECC. This approach divides the nodes into clusters, and every cluster has a cluster head that handles the encryption tasks of its group members. This approach provides the parallel execution of the nodes in the clusters without affecting the operation of the other nodes and the cluster heads. Sadhukhan et. al. in [91], presented a remote user authentication scheme with the help of the ECC protocol. This approach operates in three phases registration, log-in, and the session key negotiation phase. This approach tends to provide authentication of users and privacy of data. In [92], the researchers present a lightweight authentication scheme for healthcare devices. This approach makes use of the simple hash primitives with the XoR operations to authenticate the users in the medical application. This approach tends to provide secure sessions to the registered and verified users in the healthcare network. The authors in [156] present the use of the polynomial multiplication technique which is a technique of quantum cryptography which employs the use of the mechanisms like negating and swapping to detect faults in the data sub blocks. The authors in [157] present the use of an authentication mode, the Galious Counter Mode (GCM) in the AES algorithm that is capable of detecting faults in structure dependent as well as structure independent architectures with single or multi bit signatures. In [158], the researchers present the post quantum cryptography approach named SABER which is flexible cryptographic scheme and the FALCON which is a signature based method for detecting fault attacks and these approaches present low overheads.

Table III lists the summary of the discussed lightweight cryptography solutions with the advantages and limitations and the details of implementation tools

TABLE III: SUMMARY OF LIGHTWEIGHT CRYPTOGRAPHY SOLUTIONS

Ref.	Description	Security Layer	Advantages	Limitations	Tools Used
[80]	DES algorithm consisting of 16 rounds with 64 bits of plain text block	Network Layer	Easy to Implement	The high computational overhead compared to other LWC algorithms	Matlab Simulator
[82]	AES algorithm with 128-bit key size along with shuffling and segmentation used for securing agricultural data	Network Layer	Reliable and more secure compared to DES	High computation cost	Implementation Tool Not Specified
[83]	Using substitution technique based on Fiestal structure for the encryption process	Network Layer	Less computational time	Key management needs to be done effectively	Matlab Simulator
[84]	Applying the ECC algorithm with dynamic curves for the vehicular data transmission	Perception Layer	The less computational time for smaller key size	Takes high time for larger key sizes	C Programming on R-Pi 3B Platform
[85]	Use of RC4 and logistic maps for securing the data in the unsecured channels	Perception Layer	Less computational time	Key exchange is to be done securely which is troublesome	Python Programming on Python 3.7
[86]	Use of XOR and one-way hash function In	Application	Less communication and	Easy to crack due to the	AVISPA

	wearable devices for authenticating users	Layer	computation overhead	usage of simple hash XOR functions	Security Analyzer Tool
[87]	Use of group signature and hash function for authentication of the nodes in wireless sensor networks	Network Layer	Hard to crack due to the complex computations involved in hash calculations	Complex calculations and changing of group keys will be difficult in resource-constrained devices	Matlab Simulator
[88]	Ultra-lightweight block cipher technique making using bit slicing and WTS method	Perception Layer	Less computation time due to the use of less complex functions	Storage requirements demand more resources	Arduino UNO platform
[89]	Use of ECC and AEAD ciphers to achieve confidentiality, authentication, and integrity	Application Layer	Difficult for the crypt-analyst to break the cipher text	High computation time compared to other techniques	Implementation details not provided
[90]	CoopECC: optimized ECC approach by dividing nodes into clusters and cluster head initiating ECC encryption	Application Layer	Less overhead on the nodes because of management by the cluster head	Election of cluster head is a time-consuming process	Telosb sensors, NesC and TinyOS, and Tossim Simulator
[91]	Remote user authentication scheme with ECC encryption	Application Layer	Less communication and storage cost	Higher Computation time compared to other related schemes	AVISPA security analyzer tool
[92]	Use of Simple Hash and bitwise XOR and nonce for user authentication.	Application Layer	Less communication and computation costs	Due to less complex iterations, crypt-analysis may be easy	AVISPA security analyzer tool

B. Fog Computing Solutions

Fog computing is the emerging computing paradigm that tries to bring the processing power of the cloud closer to the IoT devices in the AAL systems by providing an intermediate layer between the devices and the Cloud [93]. The Fog computing paradigm tends to lessen the load on the cloud of data processing by allowing the processing of the data at the intermediate layer which results in lower latency and improved QoS [48]. It provides scalability in the network and is often used in time-sensitive applications. As the processing of the data occurs nearer to the devices, the security can be better achieved due to less amount of data transferred to the cloud and the reduced latency. The introduction of the Fog layer comprising of Fog devices provides a platform to implement the complex security solutions which were difficult to implement directly on the cloud [94]. The computation and the processing tasks are handled by the Fog layer which were previously handled by the cloud. The architecture of the Fog computing paradigm in IoT networks is shown in Figure 3.

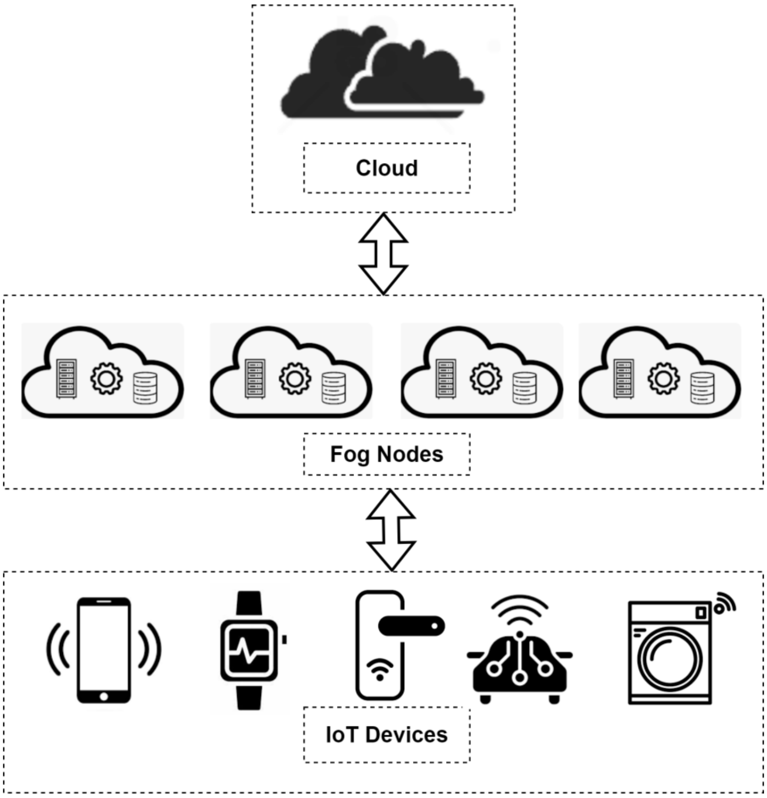

Fig. 3. Fog Computing Paradigm in IoT

In [93], the authors presented a security solution to tackle the impersonate attack in IoT by securing the communication channels between the IoT devices and the Fog nodes. The researchers described the use of the self-learning model on the Fog nodes at the Fog Layer. The authors aim to detect the anomalies during the data transfer at the Fog Layer. Alrawais et. al in [95] presented the attribute-based encryption scheme at the Fog layer to ensure secure communication between the IoT nodes and the Fog Nodes. The authors in this paper aim to provide confidentiality and integrity. They also present the application of digital signatures at the Fog layer for authentication purposes.

In [96], the authors show the scheme for revoking the certificates before the expiration time. The authors make use of the Bloom filters for verifying the certificates of the other devices in the networks. The authors claim to provide the authentication of the user with the help of certificates and focus on the proper revocation of the certificates at proper time intervals at the Fog Layer. Alharbi et. al in [97] presented the FOCUS system for implementing the challenge-response mechanism for the authentication of the users. This paper also presents the use of the virtual private network to secure communication channels among the devices. The authors in this paper aim to provide the authentication of users and confidentiality of users.

Fu et. al. in [98] presented a framework that is designed for the time-sensitive application. The data of the time-sensitive applications is processed at the Fog Layer and the data of time-insensitive applications is sent to the cloud for processing. This approach aims to reduce the latency and avoid the stealing of data by the attacker during the communication to the cloud. This paper targets to achieve the confidentiality of data in the network. Li et. al [99], presented an encryption approach where the management of keys and the complex procedure of cryptography is performed at the Fog. This approach presents the attribute-based encryption scheme which presents the attribute revocation at the Fog Nodes. It tends to achieve the confidentiality of data. Gope et. al in [100] presented lightweight authentication protocols at the Fog layer. This approach makes use of exclusive OR operations and one-way functions to authenticate the users. The author also presents the key management scheme to properly manage and distribute the keys among the users.

Hu. et. al. in [101] presented a biometric-based security framework encompassing facial verification at the Fog Layer. This approach makes use of the session keys for the encryption and decryption of facial features transferred between the IoT devices and the fog nodes. The authors aim to provide confidentiality and Integrity of data during the transfer between the IoT devices and the Fog devices. In [102], the authors present an Intrusion Detection System for detecting the manin- the-middle attack in the IoT network. The anomaly-based detection approach is employed which makes use of the AES algorithm for encryption and the use of the Diffie Hellman Key Exchange algorithm for distributing the keys between the communicating parties. Diro et. al. in [103] present an IDS making use of Elliptical Curve Cryptography in the publisher-subscriber model implemented at the Fog Layer. This approach tends to provide confidentiality and Integrity with the help of the asymmetric approach providing strength in encryption. Table IV shows the summary of the Fog Computing approaches for securing IoT applications. The advantages and limitations of the approaches are also discussed. The implementation tools for different approaches are also mentioned in Table IV.

TABLE IV: SUMMARY OF FOG COMPUTING SOLUTIONS

Ref.	Description	Security Layer	Advantages	Limitations	Tools Used
[93]	Provides security of the channels between the IoT nodes and Fog nodes	Perception Layer	Data theft and Data corruption rate is low	High computational overhead	Implementation Tool not specified
[95]	Use of attribute-based encryption to secure the data communication and use of digital signatures for authentication purposes	Network Layer	Encryption algorithm has a dependency on attributes of data and not only key	High computational overhead	Python with PyCharm Cryptography library
[96]	Uses the Bloom's Filter for verifying and revoking certificates	Network Layer	Low Communication Overhead	High computational overhead	Implementation details not provided
[97]	Employs a virtual private network with a challenge-response authentication mechanism to secure the communication channels	Perception Layer	Low response time	More overhead in configuring the VPN	Local Server with Pyloris Software, Remote Server implemented in Azure Cloud
[98]	Processing of data at the near layer to reduce latency in the time-sensitive applications	Network Layer	Reduces Latency	Not feasible for time-insensitive applications	Implementation tools not provided
[99]	Attribute-based Encryption technique for user and attribute revocation	Network Layer	Less dependency on the key and data for encryption	High computational overhead	Java Programming language
[100]	Lightweight authentication scheme employing exclusive operations and one-way function for authentication at Fog layer	Perception Layer	Less computational overhead due to less complex operations	Performing cryptanalysis is easy due to simple calculations.	Java Cryptography Extension on HTC One X Android smartphone as a test-bed
[101]	Encryption of the facial features transferred between the IoT nodes and fog nodes with the help of session keys	Network Layer	Less overhead due to single-key encryption	Transfer of keys is difficult and session key lifetime is to decide precariously	Implementation details not provided
[102]	Anomaly-based intrusion detection system making use of AES algorithm for encryption and Diffie Hellman Key Exchange Algorithm for key exchange	Network Layer	High accuracy due to the high number of rounds and high key size	High computational overhead	Omnet++ Simulator
[103]	ECC encryption at the Fog Nodes using Publisher Subscriber Model	Application Layer	Low computation time compared to other asymmetric approaches	High storage cost	Implementation details not provided

C. Edge Computing Solutions

Deploying the processing nodes close to the IoT devices results in better QoS and low latency. Edge computing is the technology working in a similar direction. Edge computing refers to providing the computational resources of IoT devices [104]. Thus with the help of edge computing, the data of the IoT nodes is processed at the device itself, and then the processed data is forwarded to the cloud [105]. The architecture of Edge Computing is demonstrated in Figure 4. As the processing of the data occurs at the device end, the security of the data and the devices can be better managed as the data is not sent to the cloud directly. Edge computing offers the same services as that fog Computing; the only difference is the position of the processing devices, which are placed near the IoT devices in Edge computing and somewhat far from IoT devices in the case of Fog

Computing [48]. Many researchers have designed security approaches for securing IoT with the help of Edge Computing which is discussed in this section.

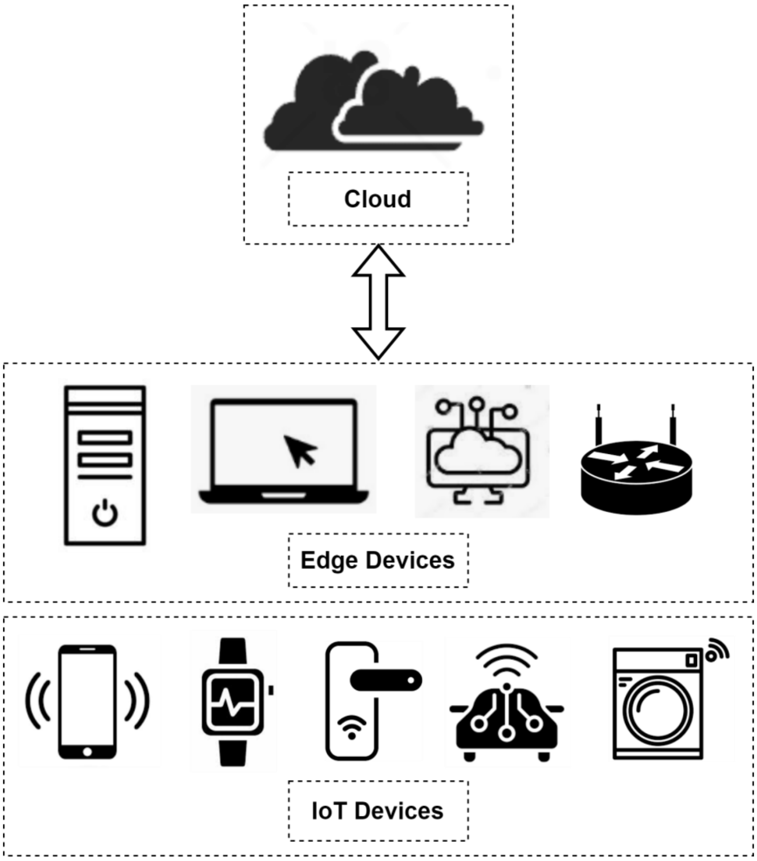

Fig. 4. Edge Computing Paradigm in IoT

Montera et al. in [106] presented an approach where a trusted virtual terminal is deployed for publishing the security policies, and the users, to access the IoT resources, need to access them according to the security policies. This approach tends to provide authentication of the users. Goldman et al. in [107] presented a channel security approach for remote attestation and server validating at the edge layer. This approach makes use of the Trusted Computing Group (TCG), which generates the signature for the state of the system, which is then logged into the event registers. This approach aims to secure the communication channels which connect the devices with the other devices. The authors in [109] present an attribute-based encryption approach at the edge layer. This approach tends to provide access to the resources to legitimate users, and there is no need to transfer the key through secure channels as the key depends on the other attributes.

In [110], the researchers present a reconfigurable security framework that includes an encryption-based approach where the Security Agent takes care of the encryption process that performs all the necessary cryptography computations. This approach makes use of the dynamic update of the security policies when required during the IoT operation. Cui et al. in [111] discussed an authentication scheme for vehicular networks where the Roadside Unit verifies the authenticity of the vehicles with the help of ECC cryptography and Fuzzy logic. Some devices at the Edge layer collaborate with the Roadside units to perform authentication tasks. This reduces the burden on the roadside units. Wazid et al. in [112] presented a device authentication approach through the edge node. This approach makes use of ECC cryptography and simple XOR operations for authentication purposes. It also involves the trusted authority for key management purposes.

Zhang et al. in [113] presented a virtualization technique where the edge nodes are virtually partitioned into multiple virtual networks. The approach aims to protect the network's communication with the help of logically partitioning the edge nodes, which becomes difficult for the attackers to attack at the edge level. In [114], the authors present a software-defined perimeter approach around the edge nodes. This approach tends to provide the authentication of the edge nodes with the help of the software controller. Thus the authentication tasks are performed at the edge nodes, which are controlled by the software controller. Wang. et al. in [115] presented a trust mechanism to establish trust with the help of edge nodes in IIoT. The trust value depends on real-time monitoring and the feedback the users provide. The approach aims to deliver trusted services to industries operating through IoT with the help of edge nodes. In [116], the researchers present a secure framework for the mobility of IoT devices with the help of Edge nodes. This approach provides confidentiality and Authentication by combining public key and symmetric encryption. Table V lists the edge computing approaches summary with the advantages and implementation tools.

TABLE V: SUMMARY OF EDGE COMPUTING SOLUTIONS

Ref.	Description	Security Layer	Advantages	Limitations	Tools Used
[106]	Use of Trusted Virtual Terminal for authentication of nodes	Network Layer	Less computation time	Scalability is an issue at the Trust terminal due to a large number of devices	OpenJDK RE 1.7.0 55 with Linux Operating System
[107]	Remote attestation and use of TCG for the security of communication channels	Perception Layer	Less computation cost and link failures are handled efficiently	Not Suitable for a large number of devices	Implementation details not provided
[109]	Proxy-aided cipher text attribute-based encryption at the Edge Layer	Application Layer	Key distribution does not require any secure channels	Computation Cost is high	Charm framework, the Python package, and the PBC library
[110]	Re-configurable security Framework employing Encryption at the Security Agent	Perception Layer	Dynamic Security Policy update.	Overload on Security Agent, Cost will be high	Hardware devices: PC and Smartphone, Software written in Java Language
[111]	Authentication mechanism based on ECC algorithm and Fuzzy logic In vehicular networks	Network Layer	Less road on Roadside units as the edge layer also contributes to computation tasks	High computation cost compared to symmetric approaches	3.4GHZ core i7 machine and using MIRACL library
[112]	Device Authentication through Edge node	Network Layer	Low computation and Communication cost	A large volume of data on TA and Trusted Authority can be attacked	NS-2 Simulator
[113]	Partitioning the nodes into the virtual network and offering edge-level services from different virtual networks	Network Layer	Easy Management due to the virtualization of edge nodes	Computation Cost is high	Eclipse, Java Programming language
[114]	Authentication is performed at Edge nodes which are controlled with the help of software perimeter	Network Layer	Reconfiguration of security patches is very easy	High overhead on the software controller managing the edge nodes	Open air interface (OAI), Waverley Labs Open SDP project
[115]	Trust mechanism based on real-time monitoring and customer feedback	Application Layer	Computation is easy	Monitoring of data requires high resources	Matlab simulator
[116]	Combination of symmetric and asymmetric encryption at edge nodes to provide secure mobility to IoT devices	Application Layer	Crypt-analysis is difficult	High computational cost	CloudSim simulator

D. SDN Solutions

Software-defined Networks are an emerging networking approach where the control planes of the routing devices are shifted to the controller, and the forwarding devices are left with the data planes only [117]. In SDN, forwarding devices like routers and switches are not to make the routing decisions. We can say that the intelligence from the networking devices is shifted to the SDN controller, and the routers need to just forward the data as per the rules decided by the controller [118]. The use of the SDN controller for making routing decisions by observing the topology provides an excellent opportunity to detect the misbehavior of the nodes in the network. The architecture of SDN is described in Figure 5. The architecture of the SDN consists of two essential layers, the forwarding layer, and the control layer. The forwarding layer comprises the forwarding devices like routers and switches. The control layer consists of the SDN controller. The controller analyzes the network topology and generates the rules for forwarding the data sent to the forwarding devices [119]. The forwarding devices forward the data packets based on the rules given by the controller. If the forwarding device does not find a rule for the data packet forwarding, it requests the SDN controller to send the rule for forwarding the data packet. Thus with the help of the SDN controller making the routing and control decisions, the anomalies can be reduced to a greater extent in the network. Many researchers have contributed to securing IoT with the help of software-defined networks.

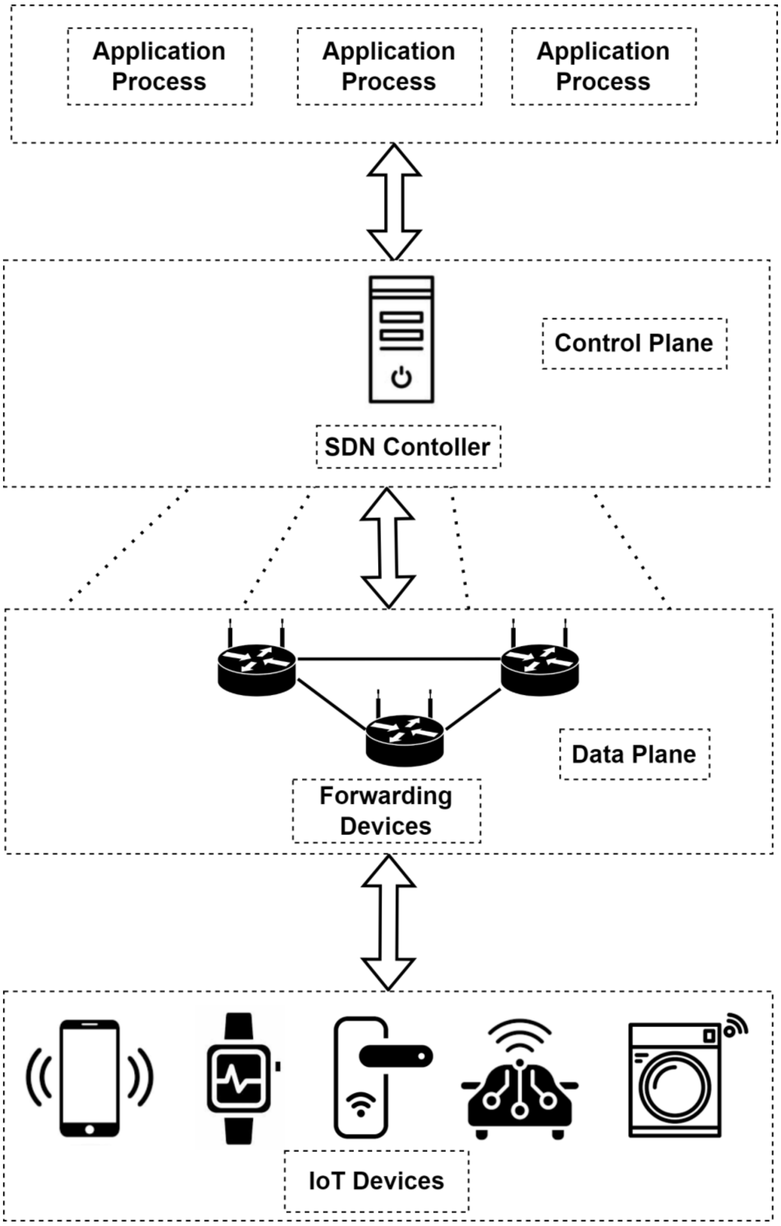

Fig. 5. SDN architecture for AAL Systems

Karmarkar et al. in [120] presented a secure architecture for IoT which employs lightweight protocol for authentication of the nodes using SDN. This approach makes use of the ECC protocol for authenticating the nodes in the network. It also presents the dynamic policy enforcement by the controller on the nodes based on which the data is routed. Liu et al. in [121] presented a secure approach for transmitting data using SDN by introducing middleboxes that manage the data flow. This approach solves issues like placing middleboxes and determining data flow to design policies effectively. This paper presents the use of the Integer Linear Program to select the optimum route, which overcomes the constraints of the switches, like the high data volumes and load balancing. In [122], the authors present the use of SDN for accessing packet-level information by implementing a firewall for securing Fig. 5. SDN architecture for IoT home devices. This paper describes the use of SDN to block the horizontal port scanners that create the botnets for home devices.

The authors in [123] present an identity-based authentication scheme that employs the ECC algorithm where the controller generates the certificates for the nodes by generating public keys for the nodes. In [124], the authors present a secure framework for the cloud IoT by deploying an end-to-end security framework with the help of SDN. This approach makes use of the index weight learning technique, which employs analytic processes and weight means for different indicators to enhance the security of IoT applications in the cloud. Sharma et al., in [125], present a secure SDN-based architecture for Smart Homes which tends to resolve the packet dropping at the forwarding devices when the controller is busy generating rules i.e., this approach safeguards against saturation attacks. The data forwarding devices are employed with the buffer for storing the packets for whom the controller generates the policies. This will prevent data loss, and thus, saturation attacks will be avoided. In [126], the authors proposed a role-based security architecture that employs different controllers for different tasks like a dedicated controller for generating keys, and another for performing cryptography. The proposed system aims to reduce the overhead on the SDN controller and avoid a single point of failure. The load balancing is also performed in the case of a heavy burden on the controller, which is effective in detecting flooding and sleep depreciation attacks.

Meng et. al. in [127] presented an SDN-based secure authentication mechanism in the healthcare sector. The patients are provided with virtual machines by the controller. The controller verifies the authenticity of the patients by verifying the unique MAC addresses of the virtual machines assigned to the patients. In [128], the authors present a privacy-preserving communication scheme between smart devices in the home. This approach employs the implementation of the lightweight authentication and encryption algorithm at the SDN controller, and all the communication happens through the controller between the devices. Iqbal et. al. in [129], present a lightweight authentication scheme in SDN-enabled smart homes. In this method, the controller assigns the unique session identifier to nodes in the network and the controller uses this identity of the node and the time difference between the request of authentication and reply to authentication. In [130], the researchers present an SDN-based secure IoT framework in which the communication of the data between the IoT devices is routed through the controller. The approach aims to prevent man-in-the-middle attacks. Table VI lists the overview of the SDN approaches with the pros and cons and the implementation details.

TABLE VI: SUMMARY OF SDN SOLUTIONS

Ref.	Description	Security Layer	Advantages	Limitations	Tools Used
[120]	Dynamic Policy enforcement by the Controller on the forwarding devices and use of ECC protocol for authentication purposes	Network Layer	High Throughput	High computation overhead	Mininet emulator, ONOS SDN Controller
[121]	Use of middleboxes for the secure transmission of data by optimizing the data volumes at switches	Perception Layer	Lower Latency	Trust issues persist at the middle-boxes	PoX Controller and Open Switches
[122]	Implementing a Firewall that prevents botnets by detecting horizontal port scanning using sampling techniques	Network Layer	Low network overhead and easy setup	Higher cost for ISP services	The simulator tool is not specified
[123]	Certificate Generation using the ECC algorithm. Trusted CA deployed on SDN controller	Network Layer	Better key management	Scalability is difficult	AVISPA security analyzer tool
[124]	End-to-end secure framework for Cloud application with the use of index weight learning technique to train the indicators	Application Layer	Better performance due to self-learning approach	Requires high computational time	Implementation details not specified
[125]	Secure framework for home applications preventing the saturation attacks which result due to overload on the controllers	Network Layer	Prevents packet overflow at the forwarding devices	High computational overhead	POX controller, Simulator used is not specified
[126]	Role-based controllers use separate controllers for different roles	Application Layer	Low overhead on the controllers	A large amount of data transfer between controllers	Implementation details not specified
[127]	Authenticating patients with the help of MAC address of virtual machines and verifying at the SDN controller in the healthcare sector	Network Layer	Availability of resources is well handled	Faces Scalability issues	POX controller and Mininet emulator
[128]	Lightweight cryptography algorithm for authenticating the smart home devices and preserving the privacy of data through cryptography between devices and SDN controller	Network Layer	Less computation time	Faces Scalability issues	Testbed: HTC One X, T1 MSP430 microcontroller and Intel Core i7-4510U laptop
[129]	A lightweight authentication protocol for the authentication of smart home devices operating	Network Layer	Less computation time	Works well for less number of devices, with	ProVerif Simulator and

	through SDN			High overloads on the controller for a large number	Burrows Abadi-Needham (BAN) logic for testing
[130]	Communication of data from one device to another through SDN controller resulting in avoidance of man-in-the-middle attack	Network Layer	Easy to implement	Heavy overload on the SDN controller can result in high congestion	Raspberry Pi and Kodi Media Center. Programs are written in C language

E. Blockchain Solutions

Blockchain is a distributed ledger that contains the transactions performed between the nodes of the network [131]. The reason for the popularity of Blockchain technology is the immutability feature where the transactions once written to the ledger, cannot be changed [132]. Blockchain operates in a distributed environment like peer-to-peer networks [48]. Blockchain was used for the security of cryptocurrencies, but now blockchain technology has been used in most applications. Blockchain refers to the immutable chain of data blocks in a sequential fashion similar to a linked list [133]. The integration of Blockchain in IoT overcomes various issues of IoT like reliability, readability, security, etc. [132]. The Blockchain is popular because of its distributed nature which involves all the nodes in deciding whether to append the block in the chain or not, which is referred to as the consensus mechanism. In the consensus mechanism, the union of data is added to the Blockchain when the majority of the nodes in the network agree on the decision to add the block [134]. Once the block is added to the chain, it cannot be changed, and the blocks in the chain are easily traceable. The overview of Blockchain is demonstrated in Fig 6. There are two types of Blockchain, namely public Blockchain, which is also known as the permission-less Blockchain, and private Blockchain, which is also known as permission-oriented Blockchain [132]. Many researchers have designed Blockchain solutions to secure IoT applications, some of which are discussed in the below paragraphs.

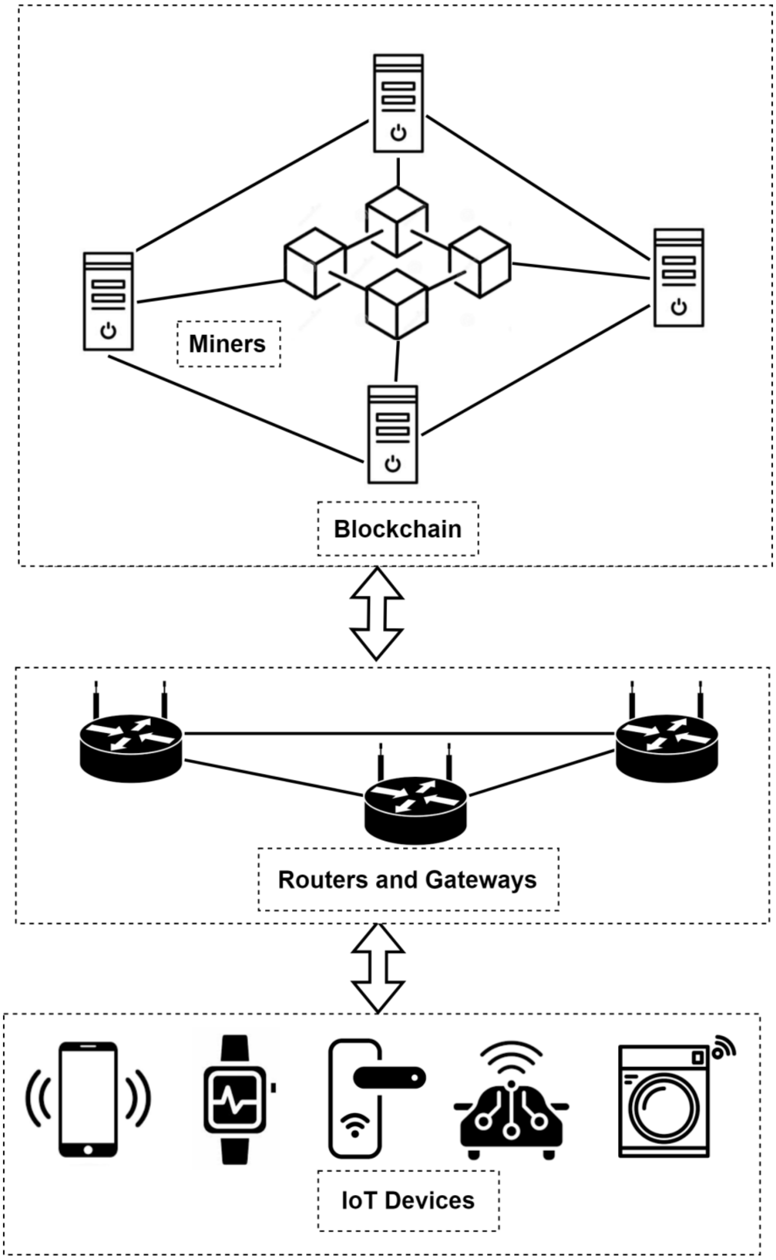

Fig. 6. Blockchain architecture for AAL Systems

Blockchain is a distributed ledger that contains the transactions performed between the nodes of the network [131]. The reason for the popularity of Blockchain technology is the immutability feature where the transactions once written to the ledger, cannot be changed [132]. Blockchain operates in a distributed environment like peer-to-peer networks [48]. Blockchain was used for the security of cryptocurrencies, but now Blockchain technology has been used in most applications. Blockchain refers to the immutable chain of data blocks in a sequential fashion similar to a linked list [133]. The integration of Blockchain in IoT overcomes various issues of IoT like reliability, readability, security, etc. [132]. The Blockchain is popular because of its distributed nature which involves all the nodes in deciding whether to append the block in the chain or not, which is referred to as the consensus mechanism. In the consensus mechanism, the union of data is added to the Blockchain when the majority of the nodes in the network agree on the decision to add the block [134]. Once the block is added to the chain, it cannot be changed, and the blocks in the chain are easily traceable. The overview of Blockchain is demonstrated in Fig 6. There are two types of Blockchain, namely public Blockchain, which is also known as the permission-less Blockchain, and private Blockchain, which is also known as permission-oriented Blockchain [132]. Many researchers have designed Blockchain solutions to secure IoT applications, some of which are discussed in the below paragraphs.

Fakhri et. al. in [135], applied Blockchain technology for securing IoT applications. The paper presents the implementation of the Ethereum Blockchain with the smart contracts mechanism. The algorithm involves the usage of the Elliptical Curve Digital Signature algorithm for the encryption of the data and the Ethereum is implemented in the Ethereum Virtual Machines. The authors in [136] presented a trust-based security approach using a credit-based Blockchain. This approach uses the obligation chains and forms an island of trust with the help of the three-way handshaking process based on the proof of work concept. This approach shows good performance against denial of service attacks. Xu. et. al [137] presented a lightweight Blockchain approach for service provisioning employing smart contacts and a proof of authority consensus mechanism. This approach enables the low-resource devices to access the network resources securely by implementing the smart contacts at the edge layer rather than the IoT devices having resource constraints.

In [138], the authors present a decentralized model for IoT security with the help of Blockchain. This approach presents the authentication of IoT devices with the help of the Blockchain. This approach maintains two different ledgers where one ledger operates between the IoT devices and the networks and the second ledger operates between the devices and the cloud. This approach employs the cryptography algorithm to reduce latency. Roy et. al. in [139] presented a secure transaction framework using Blockchain in IoT networks. This approach first provides the encryption of the data and then employs the proof of work consensus mechanism on the data to be transmitted among the devices. The block verification phase is introduced where the miners perform mining of the data, and after successful mining, the block is appended to the chain.

The authors in [140] presented the monitoring approach in the IoT networks using Blockchain. The approach provides authentication and access control services. This approach employs the usage of digital certificates with the help of the Blockchain mechanism employing the public key infrastructure. It makes use of the proof of concept consensus mechanism. The researchers in [141] presented a localization-based Blockchain approach for securing IoT networks from location-based attacks. This approach presents the Blockchain framework which guarantees the location of the devices that are stored in the Blockchain. It ensures the integrity of data and detects the malicious node pretending to send false location details. Rathee et. al. in [142] present the use of the Blockchain for securing healthcare applications. This approach employs the creation of the hash of the data and appending it to the Blockchain. Any attacker wishing to change the data will result in a change of the hash and this change will be visible to the entire network. Table VII presents a summary of the various approaches of Blockchain.

TABLE VII: SUMMARY OF BLOCKCHAIN SOLUTIONS

Ref.	Description	Security Layer	Advantages	Limitations	Tools Used
[135]	Uses Ethereum Blockchain with the smart contracts mechanism using ECDSA algorithm for encryption	Network Layer	Data Integrity is preserved with the help of the ECDSA algorithm	This approach requires high computation time	Golang Programming Language, Truffle Framework
[136]	Credit-based Blockchain approach using obligation chain	Perception Layer	Provides good performance against DoS attacks by presenting an environment of trust	Not capable to secure against another category of attacks	Implementation tool not specified
[137]	Uses Smart contracts and Proof of Authority consensus mechanism at the edge node Network Layer	Network Layer	The approach provides high throughput	Results in high latency and the trustworthiness of edge nodes are required	Simulated on a virtual server and virtual edge node on a laptop and Ethereum Geth 1.8.11 is sued for consensus
[138]	Uses distributed ledger between the devices and the network and between the devices and the cloud for securing the communication	Perception and Network Layer	Improved latency	Higher Computational overhead	Implementation details not specified.
[139]	Applying Blockchain-based encryption and performing mining among the blocks of data at the block verification phase	Network Layer	Provides good performance against man-in-the-middle attacks and backdoor attacks	Higher computational and communication overhead	Arduino UNO, Raspberry Pi 3, Different Sensors, Programming is done using Python language
[140]	Use of digital certificates for authentication with	Network	Works well for	High complexity due to a	Cisco

	the help of Blockchain employing public key infrastructure (PKI)	Layer	authentication and access control services	large number of calculations	environment, Cisco 2811 router, and TFTP server and writing TCL scripts, Hyper-ledger Composer REST API
[141]	Detecting the location of the nodes and adding the locations of the nodes to the Blockchain	Network Layer	Reduced Latency, Location-based attacks are detected with high accuracy	Works only for location-based attacks and is susceptible to various other attacks	Matlab Simulator
[142]	Calculating hash of the healthcare data of patients and stored in Blockchain	Application Layer	Good Accuracy was achieved in detecting malicious nodes	Higher Computational overhead	NS2 Simulator

F. Machine Learning Solutions

Machine Learning (ML), a subset of artificial intelligence, tends to provide intelligence to IoT devices, making them capable of reacting according to the environment and varied situations [22]. ML solutions enable IoT devices to cope with various security threats by adequately analyzing the network traffic, analyzing the nodes' behavior in the network, and taking corrective measures without human intervention [143]. ML techniques can be further classified into supervised, unsupervised, reinforcement, and deep learning [143]. Supervised machine learning techniques operate on labeled or structured data, whereas unsupervised machine learning techniques operate on unstructured data. Many supervised learning algorithms, such as support vector machines (SVM), Linear Regression, Decision Trees, and Naive Bayes make IoT systems safe and secure. Unsupervised machine learning algorithms like K-Nearest neighbors and K-means clustering are used to provide security in IoT systems [144]. Reinforcement learning enables the device to learn from its feedback, making it a reinforcement learning technique to operate with less data. Deep learning (DL) is the subset of machine learning based on the neural network structure, which overcomes the limitations of many machine learning algorithms. DL techniques such as Recurrent Neural Networks (RNN), Convolution Neural Networks (CNN) etc. secure the IoT system by analyzing the behavior of the IoT systems and the traffic flowing between them [145]. The below paragraphs describe the ML solutions for securing IoT systems.

Bagaa et al. [146] presented an AI-based monitoring framework for securing IoT systems. The solution presents the Intrusion detection system, which employs the once-class SVM algorithm. The approach tends to provide accuracy in mitigating denial-of-service attacks and data leakage. Zhang et al. in [147] presented a physical unclonable function-based key sharing where the keys are generated using the ML algorithm. The keys generated by PUF employing ML tend to provide easy and secure transmission of keys. Janice et. al. in [148], showed the use of artificial neural networks at the IoT gateway to secure the system from the malicious traffic flow. The approach predicted the data loss by investigating the delay between the packets sent by the nodes. The approach showed good accuracy in detecting the misbehavior of the nodes and detecting attacks like denial of service. A slightly higher computation time is observed in the approach. Bkassiny et al. [149] presented reinforcement learning for detecting security threats in cognitive radio devices without human supervision.

Han et al. in [150] demonstrated the use of the deep Q network algorithm for preventing communication threats in the AAL system. This scheme increases the signal-to-interference noise ratio to enable the secondary users to safeguard against jamming attacks. The researchers in [151] presented using the KNN, SVM, RF, and neural networks to detect distributed denial of service attacks in the AAL system. The neural networks resulted in higher accuracy compared to the different algorithms. In [152], the authors present the use of the capsule network, which is the extension of the convolution neural network to perform end-to-end traffic classification to detect malware from legitimate traffic. The classification is performed with the help of the binary classifier and the multi-class classifiers. Liu et al., in [153], presented a deep learning approach to classify software vulnerabilities. The approach uses the bi-directional LSTM algorithm for categorizing the binary vulnerabilities. Table VIII summarizes the various ML approaches for securing AAL systems. Shafiq et. al. in [154] present an hybrid framework which employs the use of the bijective soft approach for the selection of the optimum machine learning algorithm for the detection of anomalies in the IoT systems. This approach employs different algorithms for mitigating threats and ranks the algorithms based on their performance and the top rank algorithm is selected as security algorithm. In [155]. The authors present the feature selection approach named CorrAUC which employs the filtering approach for feature selection and then the bijective soft components are applied on selected features to detect the malicious traffic in the network.

TABLE VIII: SUMMARY OF MACHINE LEARNING SOLUTIONS

Ref.	Description	Security Layer	Advantages	Limitations	Tools Used
[146]	Use of SVM classifier for detecting the malicious traffic	Network Layer	Provides Good Accuracy	High Computation Time	ONOS Controller and OSM, Coding in Python Language
[147]	Generation of encryption keys using Unclonable function employing ML algorithm	Perception Layer	Provides reliability and increases hardware efficiency	High Computation Time	Zed-Board xc7z020clg484-1, Intel Core i5 processor
[148]	Use of ANN at the IoT gateway for monitoring the traffic pattern in the IoT system	Network Layer	Good accuracy for detecting misbehavior in traffic flows	Scalability issues are observed and computational time is higher	R tool
[149]	Use of reinforcement learning for detecting threats based on the feedback system	Perception Layer	Provides Good Accuracy	High Computation Overhead and requires high processing power	Implementation details not specified
[150]	Use of deep Q learning algorithm to detect jamming attacks	Perception Layer	Faster convergence rate	Requires a large amount of data for training	Implementation tool not specified
[151]	Use of SVM, KNN, and Neural networks for classifying DoS packets from normal packets	Network Layer	Higher accuracy	Requires large data for training, Presents some delay	Implemented in Python using Scikit-learn library and Keras Library
[152]	Use of the capsule network for detecting malware through end-to-end traffic classification	Application Layer	Higher accuracy compared to CNN, LSTM	High computation time and requires large data-set	Ubuntu16.04OS, Python2.7, TensorFlow1.8.0, 4-core CPU
[153]	Use of the LSTM approach for the classification of binary vulnerabilities in software	Application Layer	Good Accuracy in detecting vulnerabilities	Large data set required for training purposes	Python language and using Keras and TensorFlow

6. DISCUSSION AND FUTURE DIRECTIONS

Securing AAL systems is a challenging task as it requires not only securing the devices within the applications but also implementing end-to-end security solutions that protect all entities involved, including IoT devices, data communication, routing, resource utilization, and data analysis. In the previous sections, we discussed various categories of solutions for securing AAL systems, each with its strengths and limitations. Researchers are actively working to address the limitations and enhance different techniques to ensure comprehensive security in AAL systems.

A. Discussion

The cryptography approaches work fine for providing confidentiality, authenticity, and integrity in the network. The devices in the AAL applications are resource-constrained devices and hence the lightweight cryptography approaches serve better for securing the data and authenticating the devices. The symmetric encryption approaches are easy to implement and the computation time incurred in symmetric key cryptography is less. But has the major issue in symmetric cryptography approaches is the key management and key distribution. As the same key is sued for encryption and decryption, the task of transferring the key from sender to receiver is a challenging task. Moreover, the task of crypt-analysis is somewhat easy compared to crypt-analysis in asymmetric key cryptography. On the other hand, public key cryptography or asymmetric cryptography tends to provide high security against cryptanalysis by making use of different keys for encryption and decryption. There is no need to distribute the keys in asymmetric key cryptography as the public keys of users are known to all and the private keys are not be shared with anyone. Thus there is no issue of secret key distribution in asymmetric encryption. The problem with asymmetric encryption is that it requires high computation time for generating keys and we need a mechanism for the distribution of public keys.

The cryptographic approaches are vulnerable to side channel attacks. The attacks like the power analysis attacks as well as the electromagnetic analysis attacks are widely used for leakage of data from the modern day devices. The authors in [159], [160] present a survey on the side channel attacks and their countermeasures through use of post quantum cryptography on the standard NIST standards for cryptography. In [161], the authors present the breaking of the Crystals Kyber which is a NIST standard for public key encryption. The researchers in [162] present the implementation of the side channel attacks against the AES-GCM standard of the NIST for cryptography. A hybrid scheme of software and hardware implementation is shown in [163] which implements a field accelerator passed on post quantum cryptography. The solutions for the PQC need to be low powered in order to facilitate them on the IoT devices. The use of the lightweight security approaches in [164] can be empowered for the PQC scheme requiring less power and energy resources. Thus the lightweight cryptography approaches needs to consider the impact of the side channel attacks too.

The side channel attacks are more sophisticated due to the exploitation of the multiple side channels which result in security breaches. The attackers focus on launching the side channel attacks along with the other techniques like fault injection of adding software vulnerabilities. This mechanism of attack gives rise to new attack named combined side channel attack. The combined attacks are vulnerable for IoT systems and the corrective measures are to be implemented for such attacks on data.. Thus in order to implement the cryptographic solutions for AAL systems, the impact of Side channel and combined attacks needs to be considered and the lightweight cryptography approaches can be implemented with integration of mechanisms safeguarding the side channel attacks.

Fog computing is the new computing approach that tends to reduce network latency by performing the analysis of the data nearer to the IoT devices in the AAL systems. Thus the computation of the data is done closer to the devices in comparison to the computation done at the cloud. Therefore, the amount of data to be exchanged between the IoT devices and the cloud is reduced. The problem with the Fog computing paradigm is that fog nodes need to be trusted. In a real-time environment, multiple fog nodes need to work in collaboration, but one fog node is not aware of another Fog node i.e. it does not have any information about the other Fog nodes in the network and this causes several security harms if the Fog nodes turns out to be malicious or if the Fog node is compromised. Thus the selection of a trustworthy Fog Node is very important.

Edge computing brings the computation of the data very near to the devices compared to Fog computing, or we can say that the processing of the data is done on the devices themselves. Edge computing provides benefits from routing attacks and data theft as the data is not transferred on public channels. Moreover, the network latency is improved to a higher level than the Fog computing architecture. The problem with Edge computing is that the devices need to be equipped with a high processing power for performing computations and data analysis. The majority of IoT devices have resource constraints which makes it difficult to implement complex computation solutions. Moreover, edge devices may suffer from flooding and energy-draining attacks with the aim of depleting resources and bringing the system to a halt.

SDNs provide centralized control of the network. The controller has knowledge of the entire network topology and thus can precisely design the rules for the forwarding devices. The SDN provides the benefits of dynamically programming security policies at any time without changing the structure of the hardware devices. The load balancing can be better performed in the SDNs. The complex security solutions can be implemented at the SDN controller, and the forwarding rules can be designed with the help of the outputs of these algorithms. The use of SDN brings scalability issues. The controller has the limitation of handling a limited number of devices. With the increase in the number of devices, there arises an overhead on the controller which may result in high delays or may sometimes result in system crashes. Another limitation of the SDN approach is the single point of failure. As all the operative decisions are taken from the controller, the entire network will turn down if the controller fails. Thus the attacker may target the SDN controller with the help of malicious code injection like viruses and worms or perform denial of service attacks on the controller to prevent the controller from performing normal operations.

The Blockchain is a decentralized, distributed approach for securing IoT. The Blockchain eliminates the limitations like scalability, single point of failure, etc. associated with the centralized approach like SDN. The feature of immutability in Blockchain prevents the denial of the transaction performed by the nodes. The integrity is preserved in the Blockchain mechanism. If the attacker wants to change the contents of the data, the attacker has to change the data half of the nodes of the network storing the block of data. Thus, data manipulation becomes very difficult in the case of Blockchain technology. The limitation of Blockchain technology is that it requires high computational resources for performing the mining process. Apart from this, the privacy of the data is violated as data of the nodes are stored in the chain of blocks, and the copy of the blocks is stored on all the odes. Additionally, devices require high storage at their end to store the copy of blocks of data. Thus for the usage of the Blockchain, we need resources having high computing, processing, and storage capacities. Sometimes the feature of immutability also raises some problems when there arises the need to alter the data by the legitimate nodes in the network.

The machine learning solutions enable the IoT nodes to cope with the various security threats on their own with minimum human intervention. The machine learning algorithms perform well for monitoring the network traffic and analyzing the behavior of the devices and then predicting future action based on based action. Machine learning solutions face some problems too. The machine learning techniques require a large volume of data for training the model and much time is required for the training process. Another limitation faced by machine learning techniques is the requirement of high-power resources to process large data sets. IoT devices are resource constrained so the application of machine learning techniques in a low-resource environment may cause problems and may result in improper detection of security threats. Many machine learning algorithms work well with a single type of data and do not perform well with heterogeneous data. Deep Learning algorithms work well with heterogeneous data but they require large data sets for training purposes.

We have discussed various categories of solutions to secure IoT and AAL systems and have listed their pros and cons of them. However, every technology has various issues which need to be addressed. The below table IX lists the various security mechanism provided by every category along with the limitations of every technique.

TABLE IX: COMPARISON OF SECURITY APPROACHES AND THEIR LIMITATIONS

Technology	Security Mechanism	Security Limitations
Lightweight Cryptography	Confidentiality, Authentication, Integrity	Management and distribution of keys is an issue. High computational overheads
Fog and Edge Computing	Confidentiality, Authentication	The Fog and Edge nodes must be trustworthy
Blockchain	Authentication, Access Control	Blockchain requires high computational resources, Data privacy is an issue
SDN	Authentication, Availability, Access Control, Non-Repudiation	Scalability and Centralized architecture
Machine Learning	Access Control, Availability, Anomaly Detection	High computational complexity

A variety of AAL projects are implemented providing various technological solutions to the elderly people. The universalAAL platform is an open ended platform solving the issues of the interoperability and standardization to develop any AAL applications [165]. This platform provides an adaptable framework for various kinds of AAL services like eHealth, social services etc. The SOPRANO system presents an AAL platform which combines the use of the ontology methods with the service oriented architecture models presenting a bifurcation of various components like sensors, behavior systems, and semantic technologies [166]. This approach is tested with large scale trials in 300 homes of the European Union. This approach pay less attention towards the data security and the approaches like blockchain or cryptography can be handy. The DESROS system was developed for the betterment of hospitalized children with the aim of providing education to them in hospitals. This approach faced several security issues which were solved by SERENITY system which provides the Access control systems and the systems for ensuring confidentiality and integrity of data [167]. The authentication is implemented with help of digital signatures. This approach was implemented and tested through installation is some schools. The GAL monitoring system is implemented for AAL platforms where the remote monitoring is facilitated with the through Virtual Private Networks [168]. The IGenda project aimed to improve the life of the elderly people with the help of the sensors for vital parameters monitoring and identifying critical problems [169]. This project employs the privacy preserving techniques to ensure the privacy of data through encryption techniques. The AAL projects face some security issues where different state of the art technologies discussed above can be helpful. The evaluation of the system is done through installations in the particular environment and monitoring the performance.

B. Future directions

Fog computing reduces the load of the cloud by processing the data at the Fog layer and sending only processed data to the cloud. The Fog layer nodes need to be trustworthy for smooth operations. The application of the machine learning algorithms can help to monitor the behavior of the Fog nodes and help to predict the future behavior of the Fog nodes. The encryption approaches face the issue of key management and computational overhead as the IoT devices are having low capacity issues. The Key management can be performed at the Fog layer as the Fog devices are capable of handling the computational complexities. Thus the use of the encryption techniques can be done at the Fog layer or the edge layer.

Blockchain helps to provide a distributed mechanism to secure IoT data. Many times in the Blockchain, invalid data gets appended to the chain. As Block chains are immutable, invalid data may be permanently stored. Thus the data should be thoroughly checked before appending it to the chain. The use of machine learning algorithms with Blockchain can be a good option as machine learning techniques classifies the data before appending it to the chain by a Blockchain consensus algorithm. Secondly, Blockchain technology demands high resources, so there arises a need to have a lightweight solution for Blockchain. The blockchain can use the lightweight cryptography algorithms for authentication and identity management. The blockchain can employ the Merkie Tress for securing the integrity of the data instead of traditional blockchain. The Proof of Authority as the consensus mechanism can be a good option for the resource constrained devices. Thus the blockchain despite of requirement of large resources, by integration of different technologies with blockchain, the security of the resource constrained devices can be enhanced.

The SDN solutions face the issue of the single point of failure. So robust solutions are necessary to secure the SDN from different attacks. Machine learning algorithms tend to be a good solution for identifying malicious traffic which tends to keep the SDN controller busy. Many applications deploy multiple SDN controllers. So communication between the controllers can be secured by applying the Blockchain technique which would help to prevent attacks like denial of service. Moreover applying machine learning algorithms at the SDN controller is a good option as the machine learning techniques require high resources; so this technique instead of applying to IoT devices can be applied at the controller. On the other hand, the machine learning algorithm would better help to classify the traffic at the controller. The key management issue may be addressed by the SDN controller by deploying key generation and distribution mechanisms at the Controller.

Machine learning algorithms tend to find hidden patterns in structured data while it faces some difficulties in the discovery of patterns from heterogeneous data. Deep learning algorithms tend to be efficient for detecting predictions from highly unstructured and heterogeneous data. Machine learning solutions when integrated with SDN and Blockchain can tend to strengthen the security of the AAL systems by predicting the hidden patterns in the data communication resulting in better accurate results.

7. CONCLUSION

The presented work delves deeply into the latest security tendencies of the IoT as they pertain to ambient assisted care facilities. This study discusses the problems with the IoT, with an emphasis on the safety concerns raised by the expansion of AAL IoT. The attack taxonomy in AAL IoT is laid out in this document, along with a breakdown of the impacted layers and proposed solutions. Lightweight cryptography, Fog computing, Edge computing, Software-defined networking (SDN), Blockchain, and machine learning are only some of the methods for securing the AAL IoT network discussed in this paper. We give a comparative review of these new approaches, highlighting the benefits and drawbacks of each technique. In addition to presenting the state-of-the-art methodology, this study details several problems with those approaches. The analysis of the article provides recommendations for future research that may aid in enhancing the safety of IoT for ambient assisted living facilities.

FUNDING AND ACKNOWLEDGEMENT

This work was supported by The Gujarat Council on Science and Technology (GUJCOST), India, grant number GUJCOST/STI/2021-2022/3922. The authors would like to acknowledge the support from Pandit Deendayal Energy University, Gandhinagar, India.

REFERENCES

[1] Shivani Panchiwala, Manan Shah, “A Comprehensive Study on Critical Security Issues and Challenges of the IoT World”, Journal of Data, Information and Management, vol. 2 no.4 pp 257-278, Dec 2020.

[2] Soumyalatha, Shruti G Hegde, “Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges”, International Journal of Advanced Networking and Applications (IJANA), 2016.

[3] Shancang Li, Li Da Xu, Shanshan Zhao, “The internet of things: a survey”, Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, Apr. 2015.

[4] Asif Ali Laghari, Kaishan Wu, Rashid Ali Laghari, Mureed Ali, Abdullah Ayub Khan, “A review and state of art of Internet of Things (IoT)”, Archives Of Computational Methods In Engineering, pp. 1-19, 2021.

[5] P.P Ray, “A survey on Internet of Things architectures”, Journal of King Saud University-Computer And Information Sciences, pp. 291- 319, 2018.

[6] Alam, T., “A Reliable Communication Framework and its Use in Internet of Things (IoT)”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, Issue 5, 2018.

[7] Khanna, A., Kaur, S., “Internet of things (IoT), applications and challenges: A comprehensive review” Wireless Personal Communications, 2020.

[8] Nizetic S., Solic P., Gonzalez-de D., Patrono L., “Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future.”, Journal Of Cleaner Production, 2020.

[9] Aman A., Yadegaridehkordi E., Attarbashi Z., Hassan R., Park, Y., “A survey on trend and classification of internet of things reviews. IEEE Access, pp. 111763-111782, 2020.

[10] Swamy S., Kota S. “An empirical study on system level aspects of Internet of Things (IoT)”, IEEE Access, pp. 188082-188134, 2020.

[11] Gupta, B., Quamara, M., “An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols”, Concurrency and Computation: Practice And Experience, John Wiley & Sons, 2018.

[12] Harbi, Y., Aliouat, Z., Harous, S., Bentaleb, A., Refoufi, A., "A review of security in internet of things", Wireless Personal Communications, pp. 325-344, 2019.

[13] Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M., "IoT Privacy and security: Challenges and solutions", Applied Sciences, 2020.

[14] Lv, Z., "Security of internet of things edge devices", Software: Practice And Experience, pp. 2446-2456, 2021.

[15] Khan, M., Salah, K., "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, pp. 395-411, 2018.

[16] Hathaliya, J., Tanwar, S., "An exhaustive survey on security and privacy issues in Healthcare 4.0", Computer Communications, pp. 311-335, 2020.

[17] Rachit, Bhatt, S., Ragiri, P., "Security trends in Internet of Things: A survey", SN Applied Sciences, pp. 1-14, 2021.

[18] Mahapatra, S., Singh, B., Kumar, V., "A survey on secure transmission in internet of things: taxonomy, recent techniques, research requirements, and challenges", Arabian Journal for Science and Engineering, pp. 6211-6240, 2020.

[19] Mousavi, S., Ghaffari, A., Besharat. S., Afshari, H., "Security of internet of things based on cryptographic algorithms: a survey", Wireless Networks, pp. 1515-1555, 2021.

[20] Nandy, T., Idris, M., Noor, R., Kiah, L., Lun, L., Juma'at, N., Ahmedy, I., Ghani, N. & Bhattacharyya, S., "Review on security of Internet of Things authentication mechanism", IEEE Access, pp. 151054-151089, 2019.

[21] Soo Fun, T., Samsudin, A., "Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey", Sensors, 2021.

[22] Tahsien, S., Karimipour, H. & Spachos, P., "Machine learning based solutions for security of Internet of Things (IoT): A survey", Journal of Network And Computer Applications, pp. 102630, 2020.

[23] Kouicem, D., Bouabdallah, A. & Lakhlef, H., "Internet of things security: A top-down survey", Computer Networks, pp. 199-221 2018.

[24] Malhotra, P., Singh, Y., Anand, P., Bangotra, D., Singh, P. & Hong, W., "Internet of things: Evolution, concerns and security challenges", Sensors, 2021.

[25] Azrour, M., Mabrouki, J., Guezzaz, A., Kanwal, A., "Internet of Things Security: Challenges and Key Issues", Security And Communication Networks, 2021.

[26] Hashemi, S., Zarei, M., "Internet of Things backdoors: resource management issues, security challenges, and detection methods", Transactions on Emerging Telecommunications Technologies, 2021.

[27] Mishra, N., Pandya, S., "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review", IEEE Access, 2021.

[28] Goyal, M.,"Enhancing security in Internet of Things using authentication techniques: A review survey", Journal Of Physics: Conference Series, 2021.

[29] Aly, M., Khomh, F., Haoues, M., Quintero, A. Yacout, S., "Enforcing security in Internet of Things frameworks: A systematic literature review", Internet of Things Journal, 2019.

[30] Ghaffar, Z., Alshahrani, A., Fayaz, M., Alghamdi, A., Gwak, J., "A topical review on machine learning, software defined networking, internet of things applications: Research limitations and challenges", Electronics, 2021.

[31] Ogonji, M., Okeyo, G., Wafula, J., "A survey on privacy and security of Internet of Things", Computer Science Review, pp. 100312, 2020.

[32] Uganya, G., Baskar R., Vijayaraj, N., "A survey on internet of things: Applications, recent issues, attacks, and security mechanisms", Journal of Circuits, Systems And Computers, 2021.

[33] Abiodun, O., Abiodun, E., Alawida, M., Alkhawaldeh. R., Arshad, H., "A review on the security of the internet of things: challenges and solutions", Wireless Personal Communications, pp. 2603-2637, 2021.

[34] Sudha, K., Jeyanthi, N., "A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT)", Cybernetics and Information Technologies, pp. 50-72, 2021.

[35] Rao, V., Prema, K., "A review on lightweight cryptography for Internet of Things based applications", Journal of Ambient Intelligence and Humanized Computing, pp. 8835-8857, 2021.

[36] Muzammal, S., Murugesan, R., Jhanjhi, N., "A comprehensive review on secure routing in internet of things: Mitigation methods and trust based approaches", IEEE Internet of Things Journal, pp. 4186-4210, 2020.

[37] Shah, J., Patel, A., "Ambient assisted living system: The scope of research and development", 2018 International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC), Tamilnadu, India, 2018.

[38] Cedillo, P., Sanchez, C., Campos, K., Bermeo, A., "A systematic literature review on devices and systems for ambient assisted living: solutions and trends from different user perspectives", 2018 International Conference On EDemocracy & EGovernment (ICEDEG), pp. 59-66, 2018.

[39] Bouchabou, D., Nguyen, S., Lohr, C., LeDuc, B., Kanellos, I., "A survey of human activity recognition in smart homes based on IoT sensors algorithms: Taxonomies, challenges, and opportunities with deep learning", Sensors, 2021.

[40] Wu, M., Lu, T., Ling, F., Sun, J. & Du, H., "Research on the architecture of Internet of Things", 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[41] Nord, J., Koohang, A. & Paliszkiewicz, J., "The Internet of Things: Review and theoretical framework", Expert Systems with Applications, pp. 97-108, 2019.

[42] Patel, K., Patel, S., "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges", International Journal of Engineering Science and Computing, 2016.

[43] Tewari, A.,Gupta, B., "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework", Future Generation Computer Systems, pp. 909-920, 2020.

[44] Darwish, D., "Improved layered architecture for Internet of Things", International Journal of Current Advanced Research (IJCAR), pp. 214-223, 2015.

[45] Sharma, C., Gondhi, N., "Communication protocol stack for constrained IoT systems", 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1-6, 2018.

[46] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., McCann, J., Leung, K., "A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities", IEEE Wireless Communications, pp. 91-98, 2013.

[47] Asghari, P., Rahmani, A., Javadi, H., "Internet of Things applications: A systematic review", Computer Networks, pp. 241-261, 2019.

[48] Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., "Recent Security Trends in Internet of Things: A Comprehensive Survey", IEEE Access, 2021.

[49] Javed, A., Ahmed, W., Pandya, S., Maddikunta, P., Alazab, M., Gadekallu, T., "A survey of explainable artificial intelligence for smart cities", Electronics, 2023.

[50] Fahad, L., Tahir, S., "Activity recognition and anomaly detection in smart homes", Neurocomputing, pp. 362-372, 2021.

[51] Samizadeh Nikoui, T., Rahmani, A., Balador, A., Haj Seyyed Javadi. H., "Internet of Things architecture challenges: A systematic review", International Journal of Communication Systems, 2021.

[52] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E., "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues", IEEE Communications Surveys & Tutorials, pp. 1191-1221, 2020.

[53] Raghuvanshi, A., Singh, U., Shuaib, M., Alam, S., "An investigation of various applications and related security challenges of Internet of things", Materials Today: Proceedings, 2021.

[54] Goyal, S., Sharma, N., Bhushan, B., Shankar, A., Sagayam, M., "Iot enabled technology in secured healthcare: applications, challenges and future directions", Cognitive Internet of Medical Things for Smart Healthcare, pp. 25-48, 2021.

[55] Sobin, C., "A survey on architecture, protocols and challenges in IoT", Wireless Personal Communications, pp. 1383-1429, 2020.

[56] Maskeli¯unas, R., Damaˇseviˇcius, R., Segal, S., "A review of internet of things technologies for ambient assisted living environments", Future Internet., 2019.

[57] HaddadPajouh, H., Dehghantanha, A., Parizi, R., Aledhari, M., Karimipour, H., "A survey on internet of things security: Requirements, challenges, and solutions", Internet of Things, pp. 100129, 2021.

[58] Saputro, N., Tonyali, S., Aydeger, A., Akkaya, K., Rahman, M., Uluagac, S., "A review of moving target defense mechanisms for Internet of Things applications", Modeling And Design of Secure Internet of Things, pp. 563-614, 2020.

[59] Li, Y., Su, X., Ding, A., Lindgren, A., Liu, X., Prehofer, C., Riekki, J., Rahmani, R., Tarkoma, S., Hui. P., "Enhancing the internet of things with knowledge-driven software-defined networking technology: Future perspectives", Sensors, 3459, 2020.

[60] Frustaci, M., Pace, P., Aloi, G., Fortino. G., "Evaluating critical security issues of the IoT world: Present and future challenges", IEEE Internet of Things Journal, pp. 2483-2495, 2017.

[61] Colakovic, A., Hadzialic, M., "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues", Computer Networks, vol. 144 pp. 17-39, 2018.

[62] Ramana, K., Revathi, A., Gayathri, A., Jhaveri, R., Narayana, C., Kumar, B., "WOGRU-IDS An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks", Computer Communications, 2022.

[63] Jemmali, M., Denden, M., Boulila, W., Srivastava, G., Jhaveri, R., Gadekallu, T., "A Novel Model Based on Window-Pass Preferences for Data Emergency Aware Scheduling in Computer Networks", IEEE Transactions on Industrial Informatics, 2022.

[64] Ahmad, M., Younis, T., Habib, M., Ashraf, R., Ahmed. S., "A review of current security issues in Internet of Things", Recent Trends And Advances In Wireless And IoT-enabled Networks, pp. 11-23, 2019.

[65] Abosata, N., Al-Rubaye, S., Inalhan, G., Emmanouilidis. C., "Internet of things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications", Sensors, 2021.

[66] Grammatikis, P., Sarigiannidis, P., Moscholios, I., "Securing the Internet of Things: Challenges, threats and solutions", Internet of Things Journal, pp. 41-70, 2019.

[67] Mohanty, J., Mishra, S., Patra, S., Pati, B., Panigrahi, C., "IoT security, challenges, and solutions: A review", Progress in Advanced Computing and Intelligent Engineering, pp. 493-504, 2021.

[68]Patel, A., Chawda, K., "Blackhole and grayhole attacks in MANET", International Conference on Information Communication and Embedded Systems (ICICES 2014), IEEE, pp. 1-6, 2014.

[69] Patel, A. Jhaveri. R., "Addressing packet forwarding misbehavior with two phase security scheme for AODV-based MANETs", International Journal of Computer Network and Information Security, 2016.

[70]Patel, A., Chawda. K., "Dual security against grayhole attack in MANETs", Intelligent Computing, Communication and Devices, pp. 33-37, 2015.

[71] Jhaveri, R., Desai, A., Patel, A., Zhong. Y., "A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs", Security and Communication Networks, 2018.

[72] Mosenia, A., Jha. N., "A comprehensive study of security of internet of things", IEEE Transactions on Emerging Topics in Computing, pp. 586-602, 2016.

[73] Abbas, S., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U., Shah, G., Bakhshi, T., Cambiaso. E., "Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach", Sensors, 2021.

[74] Borrego, C., Amadeo, M., Molinaro, A., Jhaveri. R., "Privacy preserving forwarding using homomorphic encryption for information centric wireless ad-hoc networks", IEEE Communications Letters, pp. 1708-1711, 2019.

[75] Hossain, M., Fotouhi, M., Hasan. R., "Towards an analysis of security issues, challenges, and open problems in the internet of things", 2015 IEEE World Congress on Services, pp. 21-28, 2015.

[76] Thakor, V., Razzaque, M., Khandaker, M., "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities", IEEE Access, pp. 28177-28193, 2021.

[77] Patel, C., Bashir, A., AlZubi, A., Jhaveri, R., "EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element", Digital Communications and Networks, 2022.

[78] Sinha, M., Dutta, S., "Survey on Lightweight Cryptography Algorithm for Data Privacy in Internet of Things", Proceedings Of The Fourth International Conference on Microelectronics, Computing and Communication Systems, pp. 149-157, 2021.

[79] Takieldeen, F., Khalifa, F., "Authentication and Encryption of IoT Devices Based on Elliptic Curves: A survey", Journal of Intelligent Systems and Internet of Things (JISIoT), 2021.

[80] Chandi, P., Sharma, A., Chhabra, A., Gupta, P., "A DES-based mechanism to secure personal data on the internet of things", International Conference on Communications and Cyber Physical Engineering 2018, pp. 45-53, 2018.

[81] Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H., "Pushing the limits: A very compact and a threshold implementation of AES", Annual International Conference on The Theory and Applications of Cryptographic Techniques, pp. 69-88, 2011.

[82] Vidyashree, L., Suresha, B., “Methodology to secure agricultural data in IoT”, Emerging Technologies in Data Mining and Information Security, pp. 129-139, 2019.

[83] Usman, M., Ahmed, I., Aslam, M., Khan, S., Shah, U., “SIT: A Lightweight Encryption Algorithm for Secure Internet of Things”, International Journal of Advanced Computer Science and Applications, vol. 8, no. 1, 2017.

[84] Wang, J., Li, J., Wang, H., Zhang, L., Cheng, L., Lin, Q., “Dynamic scalable elliptic curve cryptographic scheme and its application to in vehicle security”, IEEE Internet Of Things Journal, pp. 5892-5901, 2018.

[85] Liu, T., Wang, Y., Li, Y., Tong, X., Qi, L., Jiang, N., “Privacy protection based on stream cipher for spatiotemporal data in IoT”, IEEE Internet of Things Journal, pp. 7928-7940, 2020.

[86] Gupta, A., Tripathi, M., Shaikh, T., Sharma. A., “A Lightweight Anonymous User Authentication and Key Establishment Scheme for Wearable Devices”, Computer Networks, vol. 149, pp. 29-42, 2018.

[87] Lee, J., Sung, Y., Park, J., “Lightweight sensor authentication scheme for energy efficiency in ubiquitous computing environments”, Sensors, 2016.

[88] Sliman, L., Omrani, T., Tari, Z., Samhat, A, Rhouma, R., “Towards an ultra-lightweight block ciphers for Internet of Things”, Journal of Information Security and Applications, pp. 102897, 2021.

[89] Seok, B., Sicato, J., Erzhena, T., Xuan, C., Pan, Y., Park, J., “Secure D2D communication for 5G IoT network based on lightweight cryptography”, Applied Sciences, 2019.

[90] Jerbi, W., Guermazi, A., Cheikhrouhou, O., Trabelsi, H., “CoopECC: a collaborative cryptographic mechanism for the internet of things”, Journal of Sensors, 2021.

[91] Sadhukhan, D., Ray, S., Biswas, G., Khan, M., Dasgupta, M., “A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography”, The Journal of Supercomputing, pp. 1114-1151, 2021.

[92] Masud, M., Gaba, G., Choudhary, K., Hossain, M., Alhamid, M., Muhammad, G., “Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare”, IEEE Internet Of Things Journal, 2021.

[93] Tu, S., Waqas, M., Rehman, S., Aamir, M., Rehman, O., Jianbiao, Z., Chang. C., “Security in fog computing: A novel technique to tackle an impersonation attack”, IEEE Access, 2018.

[94] Kuppusamy, P., Kumari, N., Alghamdi, W., Alyami, H., Ramalingam, R., Javed, A., Rashid, M., “Job scheduling problem in fog-cloud-based environment using reinforced social spider optimization”, Journal of Cloud Computing, 2022.

[95] Alrawais, A., Alhothaily, A., Hu, C., Xing, X., Cheng., X., “An attribute-based encryption scheme to secure fog communications”, IEEE Access, pp. 9131-9138, 2017.

[96] Alrawais, A., Alhothaily, A., Hu, C., Cheng. X., “Fog computing for the internet of things: Security and privacy issues”, IEEE Internet Computing, pp. 34-42, 2017.

[97] Alharbi, S., Rodriguez, P., Maharaja, R., Iyer, P., Subaschandrabose, N., Ye. Z., “Secure the internet of things with challenge response authentication in fog computing”, IEEE 36th International Performance Computing And Communications Conference (IPCCC), pp. 1-2, 2017.

[98] Fu, J., Liu, Y., Chao, H., Bhargava, B., Zhang. Z., “Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing”, IEEE Transactions on Industrial Informatics, pp. 4519- 4528, 2018.

[99] Li., L., Wang, Z., Li., N., “Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT”, IEEE Access, pp. 176738-176749, 2020.

[100] Gope, P., “LAAP: Lightweight anonymous authentication protocol for D2D-Aided fog computing paradigm”, Computers & Security, pp. 223- 237, 2019.

[101] Hu, P., Ning, H., Qiu, T., Song, H., Wang., Y., Yao, X., “Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things”, IEEE Internet Of Things Journal, pp. 1143-1155, 2017.

[102] Aliyu, F., Sheltami, T., Mahmoud, A., Al-Awami, L., Yasar, A., “Detecting Man-in-the-Middle Attack in Fog Computing for Social Media”, Tech Science Press, 2021.

[103] Diro, A., Chilamkurti, N., Kumar, N., “Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing”, Mobile Networks and Applications, pp. 848-858, 2017.

[104] Sha, K., Yang, T., Wei, W. & Davari, S., “A survey of edge computing based designs for IoT security”, Digital Communications and Networks, pp. 195-202, 2020.

[105] Chaudhary, G., Srivastava, S., Khari, M., “Generative Edge Intelligence for Securing IoT-assisted Smart Grid against Cyber-Threats”, International Journal of Wireless Ad Hoc Communication, 2023.

[106] Montero, D., Yannuzzi, M., Shaw, A., Jacquin, L., Pastor, A., Serral- Gracia, R., Lioy, A., Risso, F., Basile, C., Sassu, R. & Others, “Virtualized security at the network edge: a user-centric approach”, IEEE Communications Magazine, pp. 176-186, 2015.

[107] Goldman, K., Perez, R., Sailer, R., “Linking remote attestation to secure tunnel endpoints”, Proceedings of The First ACM Workshop on Scalable Trusted Computing, pp. 21-24, 2006.

[108] Zhang, T., Zhang, Y., Lee, R., “Cloudradar: A real-time side-channel attack detection system in clouds”, International Symposium on Research In Attacks, Intrusions, And Defenses, pp. 118-140, 2016.

[109] Cui, H., Yi, X., Nepal, S., “Achieving scalable access control over encrypted data for edge computing networks”, IEEE Access, pp. 30049- 30059, 2018.

[110] Hsu, R., Lee, J., Quek, T., Chen, J., “Reconfigurable security: Edgecomputing- based framework for IoT”, IEEE Network, pp. 92-99, 2018.

[111] Cui, J., Wei, L., Zhang, J., Xu, Y., Zhong, H., “An efficient messageauthentication scheme based on edge computing for vehicular ad-hoc networks”, IEEE Transactions On Intelligent Transportation Systems, pp. 1621-1632, 2018.

[112] Wazid, M., Das, A., Shetty, S., JPC Rodrigues, J., Park, Y., “LDAKMEIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment”, Sensors, 2019.

[113] Zhang, P., Jiang, C., Pang, X., Qian, Y., “STEC-IoT: A security tactic by virtualizing edge computing on IoT”, IEEE Internet of Things Journal, pp. 2459-2467, 2020.

[114] Singh, J., Bello, Y., Hussein, A., Erbad, A., Mohamed, A., “Hierarchical security paradigm for IoT multi-access edge computing”, IEEE Internet of Things Journal, pp. 5794-5805, 2020.

[115] Wang, T., Wang, P., Cai, S., Ma, Y., Liu, A., Xie, M., “A unified trustworthy environment establishment based on edge computing in industrial IoT”, IEEE Transactions On Industrial Informatics, pp. 6083- 6091, 2019.

[116] Almajali, S., Salameh, H., Ayyash, M., Elgala, H., “A framework for efficient and secured mobility of IoT devices in mobile edge computing”, 2018 Third International Conference On Fog And Mobile Edge Computing (FMEC), pp. 58-62, 2018.

[117] Rahman, S., Shang, F., “A Review of Software Defined-Networking for Modern Technology and Signification”, Proceedings of 9th International Conference on Software and Information Engineering (ICSIE), pp. 47-50. 2020.

[118] Younus, M., Islam, S., Ali, I., Khan, S., Khan, M., “A survey on software defined networking enabled smart buildings: Architecture, challenges and use cases”, Journal of Network and Computer Applications, pp. 62-77, 2019.

[119] Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., Uhlig, S., “Software-defined networking: A comprehensive survey”, Proceedings of The IEEE, 103, pp.14-76, 2014.

[120] Karmakar, K., Varadharajan, V., Nepal, S., Tupakula, U., “SDN-enabled secure IoT architecture”, IEEE Internet of Things Journal, 8, pp. 6549- 6564, 2020.

[121] Liu, Y., Kuang, Y., Xiao, Y., Xu, G., “SDN-based data transfer security for Internet of Things”, IEEE Internet of Things Journal, 5 pp. 257- 268, 2017.

[122] Shirali-Shahreza, S., Ganjali, Y., “Protecting home user devices with an SDN-based firewall”, IEEE Transactions on Consumer Electronics”, 64, pp. 92-100, 2018.

[123] Salman, O., Abdallah, S., Elhajj, I., Chehab, A., Kayssi. A., “Identity-based authentication scheme for the Internet of Things”, 2016 IEEE Symposium on Computers and Communication (ISCC), pp. 1109-1111, 2016.

[124] Han, Z., Li, X., Huang, K., Feng, Z., “A software defined network based security assessment framework for cloud IoT”, IEEE Internet of Things Journal, 2018.

[125] Sharma, P., Park, J., Jeong, Y., Park, J., “Shsec: SDN based secure smart home network architecture for internet of things”, Mobile Networks and Applications, pp. 913-924, 2019.

[126] Kalkan, K., Zeadally, S., “Securing internet of things with software defined networking”, IEEE Communications Magazine, 56, pp. 186- 192, 2017.

[127] Meng, Y., Huang, Z., Shen, G., Ke, C., “SDN-based security enforcement framework for data sharing systems of smart healthcare”, IEEE Transactions on Network and Service Management, 17, 308-318, 2019.

[128] Iqbal, W., Abbas, H., Rauf, B., Abbas, Y., Amjad, F., Hemani, A., “PCSS: Privacy preserving communication scheme for SDN enabled smart homes”, IEEE Sensors Journal, 2021.

[129] Iqbal, W., Abbas, H., Deng, P., Wan, J., Rauf, B., Abbas, Y., Rashid, I., “ALAM: Anonymous lightweight authentication mechanism for SDNenabled smart homes”, IEEE Internet of Things Journal, vol. 8, 9622- 9633, 2020.

[130] Al Hayajneh, A., Bhuiyan, M., McAndrew, I., “Improving internet of things (IoT) security with software-defined networking (SDN)”, Computers, vol. 9, 2020.

[131] Alfandi, O., Khanji, S., Ahmad, L., Khattak, A., “A survey on boosting IoT security and privacy through blockchain”, Cluster Computing, vol. 24, 37-55, 2021.

[132] Alamri, M., Jhanjhi, N., Humayun, M., “Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review”, International Journal Computer Science and Network Security, vol. 19, 2019.

[133] Restuccia, F., Kanhere, S., Melodia, T., Das, S., “Blockchain for the internet of things: Present and future”, ArXiv, 2019.

[134] Lu, Y., “Blockchain and the related issues: A review of current research topics”, Journal of Management Analytics, vol. 5, pp. 231-255, 2018.

[135] Fakhri, D., Mutijarsa, K., “Secure IoT communication using blockchain technology”, 2018 International Symposium On Electronics And Smart Devices (ISESD), pp. 1-6, 2018.

[136] Di Pietro, R., Salleras, X., Signorini, M., Waisbard, E., “A blockchain based trust system for the internet of things”, Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, pp. 77-83, 2018.

[137] Xu, Y., Wang, G., Yang, J., Ren, J., Zhang, Y., Zhang, C., “Towards secure network computing services for lightweight clients using blockchain”, Wireless Communications and Mobile Computing, 2018.

[138] Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., Pustisek, M., “Towards decentralized IoT security enhancement: A blockchain approach”, Computers and Electrical Engineering, pp. 266-273, 2018.

[139] Roy, D., Das, P., De, D., Buyya, R., “QoS-aware secure transaction framework for internet of things using blockchain mechanism”, Journal of Network and Computer Applications, pp. 59-78, 2019.

[140] Kostall, K., Helebrandt, P., Belluˇs, M., Ries, M., Kotuliak, I., “Management and monitoring of IoT devices using blockchain”, Sensors, 2019.

[141] Cheikhrouhou, O., Koubˆaa, A., “Blockloc: Secure localization in the internet of things using blockchain”, 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 629-634, 2019.

[142] Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R., “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology”, Multimedia Tools and Applications, pp. 9711-9733, 2020.

[143] Al-Garadi, M., Mohamed, A., Al-Ali, A., Du, X., Ali, I., Guizani, M., “A survey of machine and deep learning methods for internet of things (IoT) security”, IEEE Communications Surveys and Tutorials, pp. 1646-1685. 2020.

[144] Salam, M., “Intelligent system for IoT botnet detection using SVM and PSO optimization”, Journal of Intelligent Systems and Internet of Things, 2021.

[145] Gautam, S., Henry, A., Zuhair, M., Rashid, M., Javed, A., Maddikunta, P., “A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization”, Electronics, 2022.

[146] Bagaa, M., Taleb, T., Bernabe, J., Skarmeta, A., “A machine learning security framework for IoT systems”, IEEE Access, pp. 114066-114077, 2020.

[147] Zhang, J., Qu, G., “Physical unclonable function-based key sharing via machine learning for IoT security”, IEEE Transactions on Industrial Electronics, 7025-7033, 2019.

[148] Canedo, J., Skjellum, A., “Using machine learning to secure IoT systems”, 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 219-222, 2016.

[149] Bkassiny, M., Li, Y., Jayaweera, S., “A survey on machine-learning techniques in cognitive radios”, IEEE Communications Surveys and Tutorials, pp. 1136-1159, 2012.

[150] Han, G., Xiao, L., Poor, H., “Two-dimensional anti-jamming communication based on deep reinforcement learning” 2017 IEEE International Conference On Acoustics, Speech And Signal Processing (ICASSP), pp. 2087-2091, 2017.

[151] Doshi, R., Apthorpe, N., Feamster, N., “Machine learning DDoS detection for consumer internet of things devices”, 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35, 2018.

[152] Yao, H., Gao, P., Wang, J., Zhang, P., Jiang, C., Han, Z., “Capsule network assisted IoT traffic classification mechanism for smart cities”, IEEE Internet of Things Journal, pp. 7515-7525, 2019.

[153] Liu, S., Dibaei, M., Tai, Y., Chen, C., Zhang, J., Xiang, Y., “Cyber vulnerability intelligence for Internet of Things binary”, IEEE Transactions on Industrial Informatics, pp. 2154-2163, 2019.

//Comments References Reviewer 1

[154] Muhammad Shafiq, Zhihong Tian, Yanbin Sun, Xiaojiang Du, Mohsen Guizani, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city”, Future Generation Computer Systems, Volume 107, 2020.

[155] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques", IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, March 2021.

//Comments References Reviewer 2

[156] A. Sarker, A. C. Canto, M. Mozaffari Kermani and R. Azarderakhsh, "Error Detection Architectures for Hardware/Software Co-Design Approaches of Number-Theoretic Transform", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 42, no. 7, pp. 2418-2422, July 2023.

[157] Mozaffari-Kermani, Mehran., “Reliable and high-performance hardware architectures for the Advanced Encryption Standard/Galois Counter Mode”, Diss. The University of Western Ontario (Canada), 2011.

[158] A. Sarker, M. Mozaffari Kermani and R. Azarderakhsh, “Efficient Error Detection Architectures for Postquantum Signature Falcon’s Sampler and KEM SABER”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 6, pp. 794-802, June 2022.

[159] Canto, A. C., Kaur, J., Kermani, M. M., & Azarderakhsh, R., “Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security”, arXiv preprint, 2023.

[160] Ali, S., Guo, X., Karri, R., Mukhopadhyay, D. (2016). Fault Attacks on AES and Their Countermeasures. In: Chang, CH., Potkonjak, M. (eds) Secure System Design and Trustable Computing. Springer, 2016.

[161] Elena Dubrova, Kalle Ngo, Joel Gärtner, and Ruize Wang., “Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste”, In Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop (APKC '23), Association for Computing Machinery, New York, NY, USA, 2023.

[162] Kaur, J., Canto, A. C., Kermani, M. M., & Azarderakhsh, R., “A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard”, arXiv preprint, 2023.

[163] R. Elkhatib, R. Azarderakhsh and M. Mozaffari-Kermani, "Accelerated RISC-V for SIKE," IEEE 28th Symposium on Computer Arithmetic (ARITH), Lyngby, Denmark, 2021, pp. 131-138, 2021.

[164] Cintas-Canto, A., Kaur, J., Mozaffari-Kermani, M., & Azarderakhsh, R., “ChatGPT vs. Lightweight Security: First Work Implementing the NIST Cryptographic Standard”, ASCON. arXiv preprint, 2023.

[165] Hanke, S., Mayer, C., Hoeftberger, O., Boos, H., Wichert, R., Tazari, M. R.,Furfari, F.,.""UniversAAL–an open and consolidated AAL platform", In Ambient Assisted Living: 4. 2011.

[166] Wolf, P., Schmidt, A., & Klein, M., "SOPRANO-An extensible, open AAL platform for elderly people based on semantical contracts", In 3rd Workshop on Artificial Intelligence Techniques for Ambient Intelligence (AITAmI'08), 18th European Conference on Artificial Intelligence (ECAI 08), Patras, Greece, 2008.

[167] Antón, P., Muñoz, A., Maña, A., "Security-enhanced ambient assisted living supporting school activities during hospitalisation", Journal of Ambient Intelligence and Human Computing 2012.

[168] Felix Büsching, Maximiliano Bottazzi, and Lars Wolf, "The GAL Monitoring Concept for Distributed AAL Platforms", IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), 2012.

[169] Angelo Costa, Aliaksandra Yelshyna, Teresa C. Moreira, Francisco C.P. Andrade, Vicente Julián, Paulo Novais, "A legal framework for an elderly healthcare platform: A privacy and data protection overview", Computer Law & Security Review, Volume 33, Issue 5, 2017.