Vidhyayana - ISSN 2454-8596

An International Multidisciplinary Peer-Reviewed E-Journal

www.j.vidhyayanaejournal.org

Indexed in: ROAD & Google Scholar

Cyber Security trends in Internet, classification and analysis of Network Attacks

Parimalkumar P Patel

Assistant Professor, Khyati School of Computer Application, Gujarat University

Dr. Binod Agarwal

Eminent Professor, Calorx Teachers' University

Dr. Dharmeshkumar Bhavsar

Director & Associate Professor, Shri Chimanbhai Patel Institute of Computer Application, Gujarat University

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

ABSTRACT

The Internet of Things (IoT) is a network of embedded objects with individually identifiable identifiers and embedded software necessary for transient state communication. This study's goal is to examine specific IoT security issues relating to IoT standards and protocols that are currently in use. In this paper, we have provided a thorough evaluation that focuses on the impending security issues with IoT, identifying the hazards associated with the current IoT system, new security protocols, and security projects proposed in recent years. In the protocols and standards proposed for the upcoming IoT systems, this work gives an updated review of the IoT architecture. In accordance with IoT security needs, a comparative analysis of protocols, standards, and offered security models is presented. This study highlights the necessity of uniformity at the communication and data audit level because failing to do so exposes the hardware, software, and data to a variety of dangers and attacks. Our work demonstrates the necessity for methods that are capable of being applied to several threat vectors. This paper gives readers a glimpse into the most recent security research trends, which will help IoT security advance. By incorporating the best security features of IoT-based devices, the study outputs can benefit the IoT research community.

Keywords: Internet of Things · Lightweight IoT protocols and standards · IoT network security models

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

1. Introduction

A significant technical revolution is currently taking place throughout the whole network sector. The issue of network automation has been popular and on the rise for a while now. Internet of Things (IoT) technology supplements it and makes it possible to supply that component. The definition of the Internet of Things [1] is the inter-device ecosystem created by devices with an emphasis on three key functions: data transmission, data reception, and data processing. The Internet of Things (IoT) network was first thought to consist of regional physical devices connected to the internet for real-time data analysis. IoT has grown in scope over time, moving beyond personal computers to include industrial IoT frameworks [2]. The expansion of IoT is shown in research studies on the subject in the fields of healthcare [3], industrial settings [4], corporate analytics, and education, among others. Due to the anticipated increase in IoT devices in a diverse environment, IoT, which previously operated in limited network spaces, has updated for wide area networks as of 2019. As a result, so have the hazards associated with it. 1.1 Problems with research This study's main goal is to investigate the most recent IoT security solutions. Along with this main objective, the sub-goals include describing and identifying the most recent security concerns in the IoT. Prior to that, it's critical to address the current IoT research challenges:

Issues with heterogeneity, connection, ubiquitous nature, and security standards are listed in order of importance.

Trending technical fields such artificial intelligence, machine learning, and software-enabled networking [5, 6], as well as cluster-based fuzzy logic modules [5, 6], have emerged as the new study fields for implementing IoT. The adoption of ultra-lightweight protocols [8, 9] for both security and core functionality [10] is a noteworthy breakthrough in the IoT. IoT security research [11] spans a broad spectrum and is constantly evolving, with new vulnerabilities always being found. The main focus of today's discussions of IoT security is on access control techniques [12], temporary encryption techniques [13], hardware-specific security solutions [14], and SQL-related input-based attack measures [15]. Therefore, by presenting IoT-related security concerns, providing accurate definitions, classifying them, and looking for a current

scenario solution to address them, our research highlights the constantly evolving security views of IoT.

1.2 Research contribution

The work has been motivated to explore security concerns in IoT based devices due to diferent IoT applications. First, to understand IoT's security aspect, it is important to have prior knowledge about the infrastructure we are dealing with; thus, we have discussed IoT architecture and made a comparative analysis of protocols and standards used in IoT. Our second research contribution includes exploring all possible aspects of recent research being made in IoT security, which will prove benefcial in developing an IoT security framework. A thorough review presented in this survey focuses on prominent threats prevailing in current IoT systems, along with the latest security models profered for the IoT environment in recent years. The purpose is to defne security solutions in IoT's security requirements: confdentiality, integrity, authenticity, and trust management [16]. Our third research contribution comprises the identification and comparative analysis of prevalent protocols and standards in the IoT. We have addressed the updated innovations and standardization practices being used in IoT [17], classifcation of security issues in IoT based on the levels at which they afect the entire environment, and their relative solutions. Research fndings show that IoT security solutions are addressed by using existing encryption techniques and novel security design models. The major security issues recognized are trust and integrity of communication. It was also revealed that IoT security challenges are enhanced by combining IoT with other networks such as SDN [18, 19]. We also discovered a need for standardization at the manufacturing evel, which shows the vulnerabilities at the hardware and software levels [20]. Inspections also revealed a need for protocols competent enough to accord for over one threat vector [21, 22]. The research outcomes can help the IoT research community by integrating the safest appropriate security features in IoT-based devices. The paper is organized as follows. Section 1, as discussed, is a brief introduction to the study. Section 2 presents a literature review of recent developments in IoT. Section 3 discusses IoT architecture along with the trending protocols and standards used in IoT. Section 4 discusses Security trends in IoT in detail. Section 5 states the result and discussion of the entire research study, and Sect. 6 concludes the complete survey work.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

2 Literature review

The current industrial trend worldwide is wireless networks with embedded networking capabilities. One of the key beneficiaries of this networking domain is IoT. Through the integration of cloud services and the provision of SaaS, IaaS, and PaaS, it has significantly advanced. IoT Commercial sectors have experienced a significant market boom over the past few years as demand for smart systems increased significantly due to their broad feature set and convenient one-click access to services. Smart systems, such as AI-based smart devices, smart home automation, smart cars, smart labs, etc., make life easier, but relying too much on them frequently comes with considerable risks. A projected graph of the predicted rise of IoT devices in the near future is shown in Figure 1 based on a statista [23] report. The technical report suggests that because the protocols and standards present on IoT devices are primarily lightweight protocols [24, 25] and, on the other end, entities constituting it have more accessible access to the server [26], these devices have become the new source hotspot for intrusion activities for hackers. These present difficulties for technology because the latter's security needs are not adequately addressed.

Threat structure in IoT architecture is not observed to be confned to a specific layer [27]. The performance of IoT systems has been negatively impacted by previous network practises that integrated network security measures into IoT. We have defined the security parameter that a particular research project uses to provide a security model in relation to traditional security models. The problem with the traditional paradigm was the lack of low-powered device algorithms and the incompatibility of security tools used for IoT devices due to differences in policy and implementation methods [28]. Recent studies have suggested innovative ways to solve traditional security problems using a wide range of encryption techniques and hardware-based approaches [29].

Two algorithmic models, UDS (user-deviceserver) and USD (user-server-device), are built to assure valid authentication for resolving trust-centric threat models in Xin Zhang and Fengtong Wen's [30] unique anonymous user WSN authentication for the Internet of Things. This approach serves multiple purposes, ensuring security during the authentication process while

consuming less storage space, communicating more effectively, and processing data more quickly. The scope of the security solution offered in this work is constrained to protecting only lightweight sensor devices from well-known network layer and physical layer-based assaults. In order to deal with Port Scanning threats and other integrity-specific vulnerabilities for AI-based IoT security solutions, Mohammad Dahman Alshehri and Farookh Khadeer Hussain and colleagues [31] propose a cluster-based fuzzy logic implementation model and a secure messaging paradigm between IoT nodes where encrypted communication takes place using hexadecimal values. This work effectively provides a detection method against hostile IoT nodes that are present in the network, but this approach does not address vulnerabilities related to the data audit attack surface. This study also does not adequately address the performance analysis in relation to operational communication and computing costs.

In order to protect data sent in the IoT context from cryptographic assaults, Priyanka et al. [13] offer a multi-stage security approach using fully homomorphic encryption (FHE) and elliptical curve cryptography (ECC). On the extra data overheads produced by the procedure, there isn't enough clarification, though. An additional problem with this paradigm is its computational expense.

Munkenyi Mukhandi et al. [5] explore the unique security solution for robotic communication using MQTT and Robot Operating System protocols from an Industrial IoT perspective. This has been accomplished using two main techniques: data encryption and authentication, both of which have demonstrated their effectiveness in safeguarding communication phases. This study provides important information about the effectiveness of cryptographic techniques for safeguarding communication lines. In contrast, this study identifies a contradiction between performance measures and cryptographic operations. With key technologies like Alexa and Echo, which reject text inputs and accept voice-over orders for action in real-time, deep learning and machine learning have made their way into the IoT world. However, problems with data packet leaks have emerged, so Pooja Shree Singh and Vineet Khanna [32] propose a voice recognition application based on Mel-frequency cepstral coefcients (MFCC) for user identification and authentication deployable in the IoT environment to guarantee data integrity, confidentiality, and privacy security. This work is helpful for securing voice-enabled IoT

applications, but a major drawback is that it depends heavily on the hardware design needed for high-quality, noise-free input. Since its inception, IoT has encountered issues with access control. To solve this issue, Michail Sidorov et al. [10] suggested an unique secure ultra-lightweight RFID protocol that leverages a permissioned blockchain network coupled with encryption that is available at various access levels and is intended for inclusion in a supply chain management system. Performance analysis shows positive outcomes with lower storage costs and quick computation. Although it is anticipated that this work would have a significant impact on safe IoT devices, the whole setup cost is unknown. In order to address security concerns regarding a large number of low energy devices becoming the target of assaults, Chen et al. [33] propose an unique Low scale Denial-of-Service attack detection approach that includes Trust evaluation with Hilbert-Huang Transformation in Zigbee WSN. This work's low rate signal detection technique is helpful in reducing the attack surface. It has scalable design because it supports both cloud and edge computing IoT devices, which is a benefit, but higher storage overheads continue to be a problem. In the realm of traditional network security, intrusion detection systems (IDS) are responsible with identifying and keeping track of threat behaviours [34]. Which some proposed models, such Snort [35], Suricata [36], and Bro [37], are an extension of from an IoT standpoint. The model produced via pattern-matching monitoring is discussed by Roesch [35] and Paxson [37]. The semantic level matching of the network activity is the basis for Suricata [36]. Ironically, such models do not expressly target the IoT environment in terms of protocol analysis availability because they are created for professional use. It is intended for advanced users, not the average person who is not familiar with the technical details of the entire framework technology. GHOST [38] is a development project that challenges existing network security solutions for the IoT by putting out a radical new reference architecture for protecting home IoT environments with personalised real-time risk control. The vendor-independent embedded network environment in a smart home network gateway is a feature of this concept. The problems with this integrated paradigm include that the entire architecture continues to be at risk from assaults like impersonation attacks, ofine password attacks, and hardware-based anomaly attacks.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

3 Internet of Things: architecture

The use cases for the Internet of Things range from single-constrained node devices to substantial cross-platform deployments of embedded technology and real-time cloud systems [39]. As was previously mentioned, IoT activities are made up of three main tasks, such as transmitting, retrieving, and processing data. The Internet of Things (IoT) is a technology that consists of data interchange across heterogeneous devices that transmit information continually to other auxiliary devices.

3.1 Layered architecture

Figure 2 illustrates the multi-layer, multi-plane architecture of the Internet of Things. The Device Management section, Application Interface section, and Communication plane are its component sections. Application Interface Layer: In this layer of the architecture, there are embedded interface modules like the Arduino IDE, Raspberry Pi, sensors, actuators, and others that enable devices to communicate with the underlying architecture. By identifying the source and destination of the data, the Device Management Plane maintains the device i/o operations. Aggregator, for instance, is a centralised component that gathers data fuxed from the devices. The communication layer is an intermediary layer made up of switches and other similar network components that define the communication standards and protocols for IoT network traffic. This layer includes protocol stacks of the most recent protocols and standards that have been put in place to control network traffic throughout the entire system. In embedded IoT contexts, new, diverse communication protocols are employed. These protocols are more energy-efficient, better at managing congestion, and offer better QoS features.

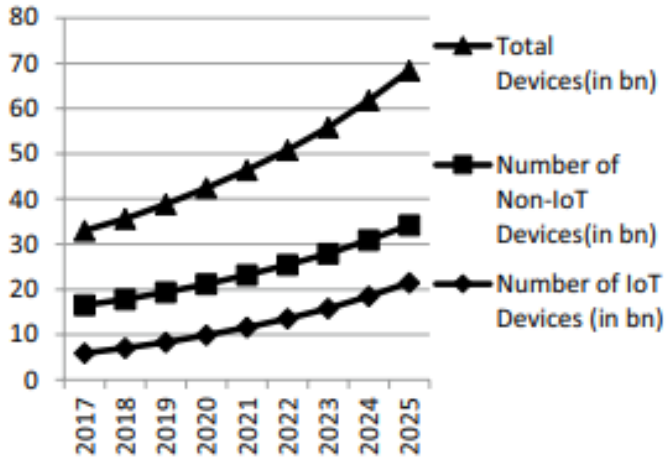

Fig. 1 Estimated census of Wireless Devices [23]

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

3.2 Communication protocols

Standard protocols like MQTT (Message Queueing Telemetry Transport), AMQP, DDS, ZigBee, and LoRaWAN [40], among others, enable communication between IoT devices. Such a setting needs a defined set of rules that initialise more easily and are compatible enough for information sharing. Notably, the IoT's communication standards include:

One of the most widely utilised protocols in the IoT ecosystem is the Bluetooth Low Energy (BLE) Protocol [41]. It is appropriate for low energy devices because of its low energy consumption capacity. Based on Generic Attributes, this protocol uses services and characteristics to carry out its operations.

2) Message Queueing Telemetry Transport (MQTT) Protocol (42), which was designed for small IoT devices and is used to send and receive data between sensor nodes. The Publisher, Broker, and Subscriber are the three main building blocks on which this protocol operates. Publisher: This component just sends data; Broker: This component is an intermediary MQTT server that analyses the data being transmitted and identifies requests for specific resources; Subscriber: This component is the component that receives messages issued by the Broker.

3) Advanced Message Queueing Protocol (AMQP) [43]: This protocol's main advantages include efficiency, portability, multichannel support, and security. This binary protocol, which is TCP-dependent, ensures authentication using SASL or TLS. It serves several purposes by enabling servers to respond to urgent requests more quickly, making it better suitable for use in multiclient scenarios.

4) Limited Application Protocol (CoAP) [44] is a protocol for constrained based environments, as its name implies. Significant traits of this protocol include its REST API-based foundation, design for smart system applications, effective congestion control, cross-protocol interoperability, and many others.

5) Data Distribution Service (DDS) protocol [45]: This Internet of Things protocol was created for M2M (Machine to Machine) communication. The publish-subscribe mechanism is used to share data, just like in the MQTT and CoAP protocols; the main distinction is that this

architecture doesn't require a broker, unlike the later two. To provide apps with high-quality QoS, it employs multicasting. Low-footprint devices can distribute DDS protocol to the cloud.

As seen, IoT protocols have offered frameworks that make it simpler to integrate IoT with other wireless technologies already in use, such as the cloud, edge computing, and lightweight embedded systems. Innovative protocols improve scalability, performance, and applicability, but they also leave security gaps that will be covered in the following section of this study. 4 Internet of Things security trends IoT is not constrained by a lack of resources, as can be seen in the sections above. The operational perspective of the IoT has expanded as a result of emerging technologies like 5G [47, 48], block chain [49], quantum computing, and edge computing being integrated with it. Figure 3 illustrates the real-world effects that new technologies have on IoT functionaries. This unstable environment is made up of heterogeneous physical objects like sensor nodes, actuators, gateways, switches, and other embedded system objects. It does not reduce the Internet of Things to networking concepts; rather, the engineering of smart devices, which forms the basis of the entire idea, has a significant impact. The newest development in IoT is self-configuring devices that use the M2M communication paradigm. Through algorithms and auxiliary technology, this configuration gives nodes the intelligence they need to make decisions for themselves under any circumstance [50, 51]. It is advantageous during rescue operations in an emergency situation where it is difficult to configure the network for a specific area with little to no assistance from damaged nodes. However, as machines are not infallible, it becomes susceptible if it depends too heavily on them. Today, adversaries specifically take advantage of weak authentication, unpatched software, and credentials for authenticity that are exposed online [52].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

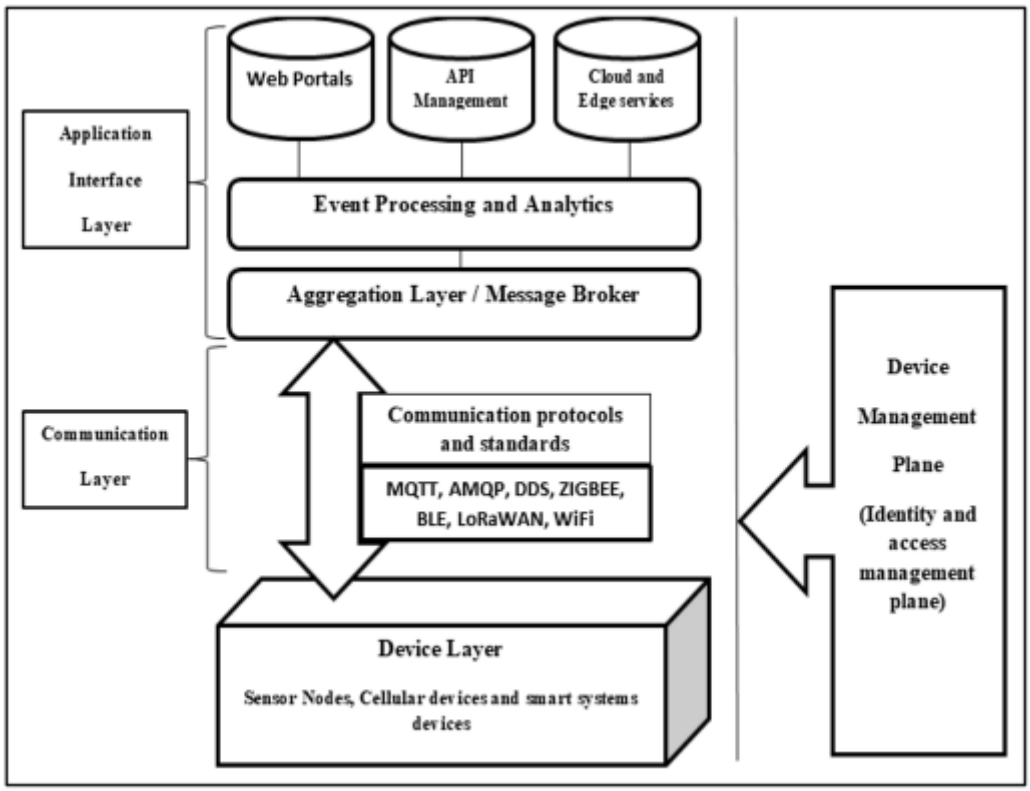

Fig. 2 Layered Internet of Things Architecture

4.1 Security challenges

1) The IoT paradigm is particularly sensitive to access requests, detecting third-party indulgence, and limited scalability compliance with security management, referring to the protocols and standards of IoT. There are a number of security issues with IoT today that relate to traditional network architecture, including: Heterogeneous Device Configuration – IoT devices interact differently with the physical world than did traditional network devices in the past. IoT devices' heterogeneous nature ramifies other networking components as they operate. NIST stressed that IoT-specific privacy regulations [53] and cyber controls must take into account the reality that IoT devices have ramifications that impact physical systems [54], ultimately affecting the physical world. Therefore, heterogeneity traits constitute a type of security concern [55].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

2) Dispersive Network Update Policy—IoT devices around the world, whether they are in a business or a person's workspace, are handled by widely dispersed servers. Such Internet of Things (IoT) devices are accessed, managed, or monitored using a different type of rule engine, and security policy is likewise different for each system component. Therefore, regularisation requires updating every device, which is a time-consuming and challenging operation for the company. Problems include a non-uniform rate of updating, additional switches leaving behind some outdated devices, or weakly confgured nodes because it takes time to maintain track of millions of nodes. The system's access control may be compromised by outside assistance in the discussed issue. Geographically scattered organisations face time- and cost-intensive problems and need to be updated and safeguarded.

IoT was never planned out for the supply of security features, hence the Add-Ins Security Policy was created. To provide secure solutions, further plugins and security controls are added to the IoT's layered architecture. As a result, unlike the traditional network paradigm, the effectiveness of security features depends on the IoT architecture's ability to function with additional resources. Client decisions about particular security options also have an impact on the effectiveness of the IoT's security.

4) Physical threats from IoT

Physical IoT setups in industrial units, network-integrated healthcare systems, and network enterprise domains all face legitimate physical security risks. Communication networks and data audit functionaries are the two main threat vectors [56]. Issues with trust management and authentication between stakeholders, network entities, and the network mode itself make up the security concerns that now plague the communication channel. Specific security problems for data audits reveal the weak security spots that existed during massive amounts of data transmission through the network and the aggregator layer of the IoT architecture. Other difficulties with physical security include the sophisticated network components being destroyed intentionally or accidentally. Physical hazards in industrial systems come from IoT devices including robotics, sensors, and hardware devices that might negatively impact the physical entities [29].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

5) Exposure threat: The IoT's endpoints, like as sensors and IP cameras located in public spaces, are the threat points that are easiest for the enemy to access. Security challenges relating to this issue lie in how architectural modifications we can make in the protocol or the communication mechanism to secure such devices against the adversaries. This results in physical-based attacks and proximity attacks, which compromise the user's authentication and integrity [57].

4.2 Classification of attacks in IoT

It is crucial to identify potential dangers in architecture based on behaviour and target set while creating security solutions. In recent years, numerous businesses have made significant financial investments to secure their IoT-based networks. IoT attacks are broken down into two components.

(1) Protocol-Based Attacks—These attacks take use of the embedded systems' inherent protocol-based architecture to affect the communication channel and forwarding channels. These are divided into several subsections. Two are protocol-based: (a) Attacks based on communication protocols—This explains the several types of exploitation that take place when nodes are in transition. Flooding attacks, key shredding attacks, and snifing attacks are a few of them. (b) Network protocol-based attacks – This illustrates how connection establishment is exploited. Wormhole attacks, Selective Forward attacks, and Snifng attacks are a few examples of attacks.

(2) Data-Based Attacks: These include dangers involving the initial data packets and messages moving across node sites. Some of its most popular security exploitations include hash collision, DoS, the development of malicious node VMs, and data disclosure.

4.2.1 Classifcation of IoT attacks based on active and passive forms

The significance of these assaults for IoT security is that certain security measures implemented to the IoT environment for active and passive attacks tend to have different effects on network performance. Modern, responsive security techniques are needed to counter active assaults in order to reduce risk and affect network performance. The effectiveness of the network is significantly less affected by passive attack protection systems, which are restricted to monitoring techniques.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

1) Denial of Service/Distributed Denial of Service Attack [58]—In terms of the Internet of Things, DDoS is the most prominent one since it affects the network's availability security parameter. In order to carry out a DDoS attack on sensor nodes or any other poorly connected nodes in a physical environment, botnets are developed. Infected packets from numerous sources travel along network data pathways after entering through these weak places, ultimately clogging up the entire link architecture and rendering servers unusable. Energy transmission industries, military communications, emergency operations, and last but not least, healthcare institutions, are all extremely risky.

2) Traffic sniffing attacks [59]—A threat activity of active data collection, traffic sniffing attacks involve the capture of vital system information that is then used for assaults like botnet attacks. With the aid of sophisticated tools, information assets such as usernames, passwords, unencrypted data information, authentication type, and hardware information are examined during such a penetration attempt. The majority of IoT devices now on the market are not sufficiently clever to counteract such threats and are therefore easily targeted by them.

3. Masquerade attack [60]: This exploit impersonates a valid access identification procedure in order to get access to target node information. Devices that have shoddy authorization procedures are highly vulnerable. By finding logical gaps in programmes or finding workarounds to the current authentication mechanism, such attacks employ stolen passwords and user credentials. The level of access that can be gained by a masquerade assault depends on the penetrator's level of authority.

Attack using Message Replay [61]:

Three methods can be used to orchestrate a replay attack: listening in on the secure communication channel between IoT devices or the gateway; intercepting the acknowledgments or connection-establishing components; and deceitfully delaying or redirecting traffic through replaying the message. The devices in the network are affected, forcing them to carry out operations that they are not supposed to, or the outcome is directed in the direction that the attacker desires. Implementation is simpler because the full message

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

may be replayed to get access to the server after packet seizing, negating the requirement for sophisticated message decryption skills.

4.3 Security solutions

In contrast to traditional security, which was tool-centric, the most recent IoT security solutions are more focused on software-centric security techniques [63]. The important security characteristics that current systems address are authentication, trust, and integrity of the communication channel among IoT devices. Even at its current state, the Internet of Things (IoT) cannot support powerful devices and is not adaptable enough to keep up with the growth of heterogeneous entities.

4.3.1 Comparative analysis of IoT protocols

IoT has additional security concerns as it integrates with other emerging technologies like SDN for greater scalability, node management, security policy, and reliability. The techniques under examination use little energy, however security concerns vary depending on several factors. The performance factor of these protocols has undoubtedly increased, but that has also shown the weak points in the guidelines.

The DTLS security mechanism is supported by the CoAP protocol, and IPSec offers ad hoc support. This still maintains security for the temporary phase, but load-based assaults like botnet and DDoS attacks continue to pose security risks [64, 65].

For secure transient periods, the MQTT protocol offers Transport layer-based security support or the Secured Socket security layer. Malicious node subscription assaults and, once more, botnet attacks present problems [62]. EnOcean's [66] special rolling code key encryption method protects the nodes in their environment. Cons include issues with code synchronisation and key confidentiality.

4.4 Comparative analysis of IoT security models

As was previously mentioned in Section 2, security models have suggested a distinctive variety of ways to secure IoT environments. The effectiveness of each solution in meeting the fundamental security needs of the IoT. In this examination, we look into the security

requirements that are met by each of the technique's parameters. Basic Confidentiality (C), Integrity (I), Availability (A), Trust management (T) among nodes, and Authenticity (A) are the security needs that have been determined here (Ay). The dual authentication model proposed by Xin Zhang and Fengtong Wen [30] excels in meeting authentication and trust security requirements through the use of UDS and USD WSN authentication models but falls short in CIA requirements, leaving it vulnerable to tracking, botnet attacks, DDoS attacks, and snooping attacks. Mohammad Dahman Alshehri and Farookh Khadeer Hussain's security proposal [31] satisfies CT security standards. However, it is still vulnerable to A, I, and Ay assaults as well as security flaws like malware, DDoS, and relay attacks. The models proposed by Munkenyi Mukhandi et al. [5] have additional provisions for authenticity in Industrial IoT environment robotic setups where encryption mechanisms are integrated using MQTT protocols. Security methods implied by Priyanka et al. [13], Munkenyi Mukhandi et al. [5, and Pooja Shree Singh and Vineet Khanna [32] have security provisions for Integrity security requirements. Strong cryptographic security techniques have been proposed by Priyanka et al. [13] to thwart Integrity-based attacks. Pooja Shree Singh and Vineet Khanna's [32] security solution relies on MFCC security coefficients to provide the needs for confidentiality and integrity security. The availability and trust security criteria in Hongsong Chen et al[33] .'s proposed model are satisfied by the Hilbert-Huang transformation, however they are exploitable in the C, I, and Ay security parameters.

5 Result and discussion

According to the comparison analysis's findings, protocol-based security solutions block the majority of IoT attack surfaces. Through the use of secured methods implemented over the Data Link and Transport layers, protocols like COAP and DDS provide effective immunity against the well-known attacks like DDoS attack and botnet attacks. In the instance of SigFOX and EnOcean, fresh protocols that prevent new threat issues like unsynchronous code definition and poor payload encryption by a special encryption method, novice methodologies are derived. The lightweight protocols MQTT and BLE have also emerged as an effective defence against dangers posed by malicious nodes and Man in the Middle attacks. There is a supply of Physically Unclonable Function [67] protocols that are ingested in the specifically developed

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

PUF chip put on the IoT devices to prevent the modifications brought in by physical attacks. Its distinctive PUF-based authentication process makes it a strong solution against threats resulting from physical assaults. Similarly, the comparison analysis for the security models is anticipated based on these protocols and standards. In order to meet the criteria for confidentiality, integrity, authenticity, availability, and trust-based security in the IoT context, security models illustrate unique uses of encryption techniques, machine learning techniques, blockchain technology, and socket programming [68, 69].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

6 Conclusion

By reviewing the recently proposed models, protocols, and encryption techniques entailed in protecting the IoT network, this work highlighted the latest security trends in the IoT network sector. Our research findings on IoT security risks highlight the expansion of the attack surface of IoT threats and vulnerabilities in protocol-based and data-based attacks, conveying the fact that traditional defences against dynamic attacks common in heterogeneous IoT environments like malicious nodes, DDoS attacks, and botnet attacks are no longer as effective as they once were. Studies of current research models reveal that the bulk of security solutions involve the use of various encryption techniques, which have been effective in securing communication channel attack surfaces in IoT while also encouraging lower energy use. The security of IoT networks has improved thanks to the integration of technologies like machine learning, artificial intelligence-based fuzzy logic methods, elliptical cryptographic functions, and blockchain. On the down side, it has made the system's overall complexity higher. The degree of openness in the purpose of security provisions has reduced as a result of the high level of abstraction of such complicated solutions. In this work, steadfast efforts that have been (and are being) made by scientific researchers worldwide in previously discussed issues have been made to address the advancement of existing communication technologies, protocols, and globally recognised standards. However, there is always room for more investigation.

References

1. Ashton K (2009) That Internet of Things thing. RFID J 22:97–114

2. Wan J, Tang S, Shu Z, Li D, Wang S, Imran M, Vasilakos AV (2016) Software-defned industrial internet of things in the context of industry. IEEE Sens J 16(20):7373–7380

3. Mavrogiorgou A, Kiourtis A, Perakis K, Pitsios S, Kyriazis D (2019) IoT in healthcare: achieving interoperability of high-quality data acquired by IoT medical devices. Sensors 19(9):1978

4. Lemayian JP, Al-Turjman F (2019) Intelligent IoT communication in smart environments: an overview. In: Artifcial Intelligence in IoT. Springer, Cham, pp 207–221

5. Mukhandi M, David P, Pereira S, and MS Couceiro (2019) A novel solution for securing robot communications based on the MQTT protocol and ROS. In: IEEE/SICE International Symposium on System Integration (SII), pp 608–613

6. Rutten E, Marchand N, Simon D (2017) Feedback control as MAPE-K loop in autonomic computing. Software engineering for self-adaptive systems III Assurances. Springer, Cham, pp 349–373

7. Sinh D, Le LV, Lin BSP, Tung LP (2018) SDN/NFV—a new approach of deploying network infrastructure for IoT. In: Wireless and optical communication conference (WOCC), IEEE, 27th, pp 1–5

8. Safkhani M, Bagheri N (2017) Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. J Supercomput 73(8):3579–3585

9. Coman FL, Malarski KM, Petersen MN, Ruepp S (2019) Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT. In: 2019 Global IoT Summit (GIoTS), IEEE, pp 1–6

10. Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH (2019) Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access 7:7273–7285

11. Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M (2020) Internet of Things (IoT) enabling technologies, requirements, and security challenges. Advances in data and information sciences. Springer, Singapore, pp 119–126
12. Wang Li, Dinghao Wu (2019) Bridging the gap between security tools and SDN controllers. ICST Trans Secur Saf 5(17):156242
13. Urla PA, Mohan G, Tyagi S, Pai SN (2019) A novel approach for security of data in IoT environment. In: Computing and network sustainability. Springer, Singaporem, pp 251–259
14. Abdul-Ghani Hezam A, Konstantas D, Mahyoub M (2018) A comprehensive IoT attacks survey based on a building-blocked reference model. Int J Adv Comput Sci Appl 9:355–373
15. Sharma K, Bhatt S (2019) SQL injection attacks-a systematic review. Int J Inf Comput Secur 11(4–5):493–509
16. Jaiswal S, D Gupta (2017) Security requirements for internet of things (IoT). In: Proceedings of International Conference on Communication and Networks, Springer, Singapore, pp 419–427
17. Radanliev P, De Roure DC, Nurse JRC, Montalvo RM, Cannady S, Santos O, Burnap P, Maple C (2020) Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci 2(2):169
18. Sood K, Shui Yu, Xiang Y (2016) Software-defned wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet Things J 3(4):453–463
19. Li Y, Chen M (2015) Software-defned network function virtualization: a survey. IEEE Access 3:2542–2553
20. Bhattacharjya A, Zhong X, Wang J, and Li X (2019) Security challenges and concerns of Internet of Things (IoT). In: Cyber-Physical Systems: architecture, security and application, Springer, Cham, pp 153–185

21. Capellupo M, Liranzo J, Bhuiyan MZA, Hayajneh T, Wang G (2017) Security and attack vector analysis of IoT devices. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, pp 593–606

22. Vervier PA, Shen Y (2018) Before toasters rise up: a view into the emerging iot threat landscape. In: International Symposium on Research in Attacks, Intrusions, and Defenses, Springer, Cham, pp 556–576

23. https://www.statista.com/statistics/471264/iot-number-ofconnected-devices-worldwide/

24. Wang K-H, Chen C-M, Fang W, Tsu-Yang Wu (2018) On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. J Supercomput 74(1):65–70

25. Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Humaniz Comput. https://doi. org/10.1007/s12652-017-0494-4

26. Grooby S, Dargahi T, Dehghantanha A (2019) A bibliometric analysis of authentication and access control in IoT devices. Handbook of big data and IoT security. Springer, Cham, pp 25–51

27. Atlam HF, Wills GB (2020) IoT security, privacy, safety and ethics. Digital twin technologies and smart cities. Springer, Cham, pp 123–149

28. Bembe M, Abu-Mahfouz A, Masonta M, Ngqondi T (2019) A survey on low-power wide area networks for IoT applications. Telecommun Syst 71(2):249–274

29. Shamsoshoara A, Korenda A, Afghah F, Zeadally S (2019) A survey on hardware-based security mechanisms for internet of things. arXiv preprint

30. Zhang X, Wen F (2019) An novel anonymous user WSN authentication for Internet of Things. Soft Comput 23(14):5683–5691

31. Alshehri MD, Hussain FK (2019) A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 101(7):791–818

32. Singh P S, and V Khanna (2019) A MFCC based Novel approach of User Authentication in IOT. In: 2nd International Conference on Emerging Trends in Engineering and Applied Science, ISSN: 2454-4248, 5(1)

33. Chen H, Meng C, Shan Z, Zhongchuan Fu, Bhargava BK (2019) A Novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang transformation and trust evaluation. IEEE Access 7:32853–32866

34. Aldaej A (2019) Enhancing cyber security in modern Internet of things (IoT) using intrusion prevention algorithm for IoT (IPAI). IEEE Access. https://doi.org/10.1109/ACCESS.2019.2893445

35. Roesch M (1999) Snort: lightweight intrusion detection for networks. In: 13th Systems Administration Conference on LISA, pp 229–238

36. (OISF), Open information security foundation: Suricata. https:// suricata-ids.org/

37. Paxson V (1999) Bro: a system for detecting network intruders in real-time. Comput Netw 31(23–24):2435–2463

38. Collen A, Nijdam NA, Augusto-Gonzalez J, Katsikas SK, Giannoutakis KM, Spathoulas G, Gelenbe E, Votis K, Tzovaras D, Ghavami N, Volkamer M (2018) Ghost-safe-guarding home IoT environments with personalised real-time risk control. International ISCIS Security Workshop. Springer, Cham, pp 68–78

39. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660

40. Gresak E, Voznak M (2018). Protecting gateway from abp replay attack on lorawan. In: International Conference on Advanced Engineering Theory and Applications, Springer, Cham, pp 400–408

41. Pallavi S, Anantha Narayanan V (2019) An overview of practical attacks on BLE Based IOT devices and their security. In: 2019 5th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, pp 694–698

42. Hunkeler U, Truong H L, Stanford-Clark A (2008) MQTT-S— A publish/subscribe protocol for Wireless Sensor Networks. In: 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), IEEE, pp 791–798

43. McAteer IN, Malik MI, Baig Z, Hannay P (2017) Security vulnerabilities and cyber threat analysis of the AMQP protocol for the internet of things. In: Valli C (Ed). The Proceedings of 15th Australian Information Security Management Conference, 5–6 December 2017, Edith Cowan University, Perth, Western Australia, pp 70–80

44. Randhawa RH, Hameed A, Mian AN (2019) Energy efficient cross-layer approach for object security of CoAP for IoT devices. Ad Hoc Netw 92:101761

45. Beckman K, Reininger J (2018) Adaptation of the DDS security standard for resource-constrained sensor networks. In: 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), IEEE, pp 1–4

46. Sethia D, Gupta D, Saran H (2018) NFC secure element-based mutual authentication and attestation for IoT access. IEEE Trans Consum Electron 64(4):470–479

47. Li S, Da Li X, Zhao S (2018) 5G Internet of Things: a survey. J Ind Inf Integr 10:1–9

48. Arfaoui G, Bisson P, Blom R, Borgaonkar R, Englund H, Félix E, Klaedtke F, Nakarmi PK, Näslund M, O'Hanlon P, Papay J, Suomalainen J, Surridge M, Wary JP, Zahariev ANDA (2018) A security architecture for 5G networks. IEEE Access 6:22466–22479

49. Mohanty SN, Ramya KC, Sheeba Rani S, Gupta D, Shankar K, Lakshmanaprabu SK, Khanna A (2020) An efcient lightweight integrated blockchain (ELIB) model for IoT security and privacy. Futur Gener Comput Syst 102:1027–1037

50. Chatterjee S, Mukherjee R, Ghosh S, Ghosh D, Ghosh S, Mukherjee A (2017) Internet of Things and cognitive radio—Issues and challenges. In: 2017 4th International Conference on OptoElectronics and Applied Optics (Optronix), IEEE, pp 1–4

51. T Leppänen, J Riekki, M Liu, E Harjula, T Ojala (2014) Mobile agents-based smart objects for the internet of things. In: Internet of Things Based on Smart Objects. Springer, Cham, pp 29–48

52. Ahmad M, Younis T, Habib MA, Ashraf R, Ahmed SH (2019) A review of current security issues in Internet of Things. Recent trends and advances in wireless and IoT-enabled networks. Springer, Cham, pp 11–23

53. Dabbagh M, Rayes A (2019) Internet of Things security and privacy. Internet of Things from hype to reality. Springer, Cham, pp 211–238

54. A Soni, R Upadhyay, A Jain (2017) Internet of Things and wireless physical layer security: a survey. In: Computer Communication Networking and Internet Security Springer, Singapore, pp 115–123

55. Yıldırım G, Tatar Y (2017) On WSN heterogeneity in IoT and CPSs. In: 2017 International Conference on Computer Science and Engineering (UBMK), IEEE, pp 1020–1024

56. Hou J, Leilei Qu, Shi W (2019) A survey on internet of things security from data perspectives. Comput Netw 148:295–306

57. Xu H, Sgandurra D, Mayes K, Li P, Wang R (2017) Analysing the resilience of the internet of things against physical and proximity attacks. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, pp 291–301

58. Salim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput. https:// doi.org/10.1007/s11227-019-02945-z

59. Stiawan D, Idris M, Malik RF, Nurmaini S, Alsharif N, Budiarto R (2019) Investigating Brute Force attack patterns in IoT network. J Electr Comput Eng. https://doi.org/10.1155/2019/4568368

60. Shen H, Shen J, Khan MK, Lee J-H (2017) Efcient RFID authentication using elliptic curve cryptography for the internet of things. Wireless Pers Commun 96(4):5253–5266

61. Na SJ, Hwang DY, Shin WS, Kim KH (2017) Scenario and countermeasure for replay attack using join request messages in lorawan, In: 2017 International Conference on Information Networking (ICOIN), pp 718–720

62. Om Kumar CU, Bhama PRKS (2019) Detecting and confronting fash attacks from IoT botnets. J Supercomput 75(12):8312–8338

63. Flauzac O, Gonzalez C, Nolot F (2016) Developing a distributed software defned networking testbed for IoT. Procedia Comput Sci 83:680–684