SMART HOME AND INDUSTRIAL IOT DEVICES: CRITICAL PERSPECTIVES ON CYBERTHREATS, FRAMEWORKS AND PROTOCOLS

Akashdeep Bhardwaj

Bentham Books

Smart Home and Industrial IoT Devices: Critical Perspectives on Cyberthreats, Frameworks and Protocols

Authored by

Akashdeep Bhardwaj
School of Computer Science
University of Petroleum and Energy Studies
Dehradun
India

Smart Home and Industrial IoT Devices: Critical Perspectives on Cyberthreats, Frameworks and Protocols

Author: Akashdeep Bhardwaj

ISBN (Online): 978-981-5256-71-0

ISBN (Print): 978-981-5256-72-7

ISBN (Paperback): 978-981-5256-73-4

First published in 2024.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

In the ever-evolving landscape of technology, the proliferation of Smart Home and Industrial IoT (Internet of Things) devices has become a defining hallmark of our era. These interconnected gadgets promise unparalleled convenience, efficiency, and automation in our daily lives and industrial processes. From smart thermostats that regulate our home temperatures to industrial sensors that optimize manufacturing processes, these devices have transformed the way we interact with our environment. They hold the power to enhance our lives and redefine our industries, but they also bring with them a complex set of challenges that demand our immediate attention.

The title of this book, "Smart Home and Industrial IoT Devices: Critical Perspectives on Cyberthreats, Frameworks, and Protocols", encapsulates the essence of our exploration into this technological realm. This book is an endeavor to shed light on the multifaceted landscape of Smart Home and Industrial IoT devices, focusing particularly on the critical perspectives that have emerged because of their proliferation.

At the heart of this book lies a crucial examination of the potential cyberthreats that have surfaced with the rapid integration of these devices into our lives and industries. The interconnected nature of IoT devices, while offering unparalleled convenience and data-driven decision-making, also creates a myriad of security vulnerabilities. Cyberattacks on these devices can have far-reaching consequences, both at the individual level in our homes and at the industrial scale in our factories. Understanding these threats and the strategies to mitigate them is paramount in safeguarding our privacy, security, and economic stability.

Moreover, this book delves into the frameworks and protocols that underpin the functioning of Smart Home and Industrial IoT ecosystems. The selection and implementation of these frameworks play a pivotal role in determining the effectiveness of these devices. We explore the standards, communication protocols, and architectural paradigms that drive IoT systems, offering insights into the advantages and limitations of each approach.

The critical perspectives presented within these pages are not intended to dissuade the adoption of Smart Home and Industrial IoT devices but rather to inform and empower individuals, organizations, and policymakers. By delving into the complexities of these technologies, we can make more informed decisions, build more resilient systems, and harness the true potential of the IoT revolution.

In this book, we bring together a diverse array of voices, from cybersecurity experts to industry practitioners, to provide a comprehensive and holistic view of the Smart Home and Industrial IoT landscape. Our aim is to provide readers with the knowledge and insights required to navigate the challenges and opportunities presented by these technologies.

As we embark on this journey through the world of Smart Home and Industrial IoT devices, we invite readers to approach this exploration with a critical eye and an open mind. The future of IoT is rich with possibilities, but it is also fraught with challenges. By gaining a deeper understanding of the cyberthreats, frameworks, and protocols, we can collectively shape a safer, more efficient, and connected world for generations to come.

We hope this book serves as a valuable resource for all those intrigued by the ever-expanding world of Smart Home and Industrial IoT devices and the critical perspectives that surround them.

Akashdeep Bhardwaj
School of Computer Science
University of Petroleum and Energy Studies
Dehradun
India

CHAPTER 1

Significance of IoT for Smart Homes and Cities

Abstract: The integration of the Internet of Things (IoT) has ushered in a transformative era for both residential environments and urban landscapes, re-defining the way people live, work, and interact within them. This chapter delves into the profound significance of IoT in the realm of smart homes and cities, exploring the multifaceted impact it has on enhancing efficiency, sustainability, and quality of life. In the context of smart homes, IoT technology seamlessly intertwines household devices, appliances, and systems, creating a networked ecosystem that enables automation, remote control, and intelligent decision-making. This interconnectivity offers residents unprecedented levels of convenience, energy efficiency, and security while paving the way for innovative services like predictive maintenance and health monitoring. Extending the scope to smart cities, this chapter explains how IoT transforms urban environments into dynamic, data-driven entities. Through an intricate web of sensors, actuators, and data analytics, cities can optimize resource allocation, traffic management, waste disposal, and energy consumption. This leads to reduced congestion, improved air quality, and a more sustainable urban infrastructure. However, the integration of IoT into the fabric of smart homes and cities also raises significant challenges pertaining to data privacy, security, and interoperability. These complexities necessitate robust governance frameworks and technological solutions to ensure the responsible and secure implementation of IoT technologies.

Keywords: Internet of things, IoT, Internet of everything, IoE, Internet of vehicles, IoV, Web of things, WoT.

INTRODUCTION

According to forecasts by Thales, there will be 83 billion Internet of Things (IoT) devices worldwide by 2024, up from 35 billion in 2020 [1]. According to Indian Retailer, IoT implementations will account for 20% of all devices by 2024 [2]. With the current cloud strategy, this rapid, amazing, and unparalleled development is not sustainable. Instead, a novel computing paradigm that can handle data quickly and efficiently without compromising delivery or security is needed. Applications based on the Internet of Things are producing unprecedented amounts and types of privacy-sensitive data from the devices of billions of end users. Concerns about low latency speeds, large burst rates, and geographically dispersed sites have resulted in an alarming situation. To satisfy the ever-changing

Akashdeep Bhardwaj

demands of end users, the next generation of cloud paradigms is anticipated to be more responsive and energy efficient. In addition to IoT, the Internet of Everything (IoE) and Web of Things (WoT) are beginning to link commonplace items and gadgets to cloud-hosted service apps [3, 4].

The sustainability of cloud and smart fog delivery services is impacted by the growth of data centres, which also raises delivery costs and carbon footprints. For edge computing, Cisco came up with the phrase "fog computing". A developing IoT paradigm is fog computing technology [5]. Centralized data processing would be unable to scale up and meet the requirements of such fog environments, as fog nodes and IoT devices generate data logs, and WoT and IoE bring every object online. The solution suggested by the scientific and commercial communities to deal with the problems is fog computing. Fog leverages the actual end-user device's network sensors to gather information and enable remote monitoring. Numerous industries, including healthcare, manufacturing, retail, finance, consumer products, and communication applications, have seen a sharp increase in the use of this technology. Corporates throughout the world are frantically looking for ways to run effective applications on IoT and fog technologies.

By providing computing, application connectivity, networking, storage, decision-making, data processing, and management close to the IoT device producing the data, smart fog computing closes the business gap between cloud and IoT devices. To solve these concerns, other computing paradigms akin to smart fog computing, such as Cloud of Things, edge computing, mist computing, or cloudlets, have also been proposed. These fog computing requirements cannot be met by traditional cloud systems. Current solutions call for transmitting data for processing from the network edge IoT node to the data centre. As a result, latency increases as several IoT devices' data streams take up available bandwidth and interfere with service delivery. Because cloud computing is extended to the network's edge and reduces latency and congestion, smart fog computing has emerged as the answer to the Internet of Things. Delivery and security threats can be reduced by lowering the amount of data sent over the Internet. A standard for fog computing with an open architecture is being promoted by the OpenFog Consortium [6]. This approach suggests creating multi-layered, hierarchically distributed fog clusters with a swarm of computational clients and edge nodes. Higher-layer fog clusters gather, and process data filtered from lower levels, while each cluster handles data from a single geographic area of the device farm.

These tiers carry out distinct logical tasks like control, storage, monitoring, local operations, and business decision-making. The network, storage, and computing are extended to the network edge via this system-level architecture. To do this, data must be delivered via intelligent edge devices rather than *via* the Internet to

cloud data centres. This expedites decision-making and signifies a departure from conventional design that relies on cloud-based apps and the Internet. The following are necessary components of a successful fog computing architecture.

- Low Latency: Performance can be significantly impacted by any delays in data processing, data transmission to the cloud data centre, and data return to the application [7].
- Applications in manufacturing sector that monitor health, respond to emergencies, shut down production floors in real time, or restore electrical service must have a minimal latency of even milliseconds.
- Bandwidth conservation: Large computing and storage resources are needed for Big Data, predictive analytics, and data mining; these resources are typically found in the cloud. Noise and false positives are minimized in logs produced by IoT devices and real-time systems, such as Boeing airplanes that produce 10 TB of data in just 30 minutes of flight time or offshore oil rigs that can produce 500 GB of data in a week. Sending this much data to the cloud from hundreds of thousands of edge devices and nodes is not feasible [8].
- Data Security: Both in transit and at rest, created IoT data must be private, secure, and compliant. On the unprotected Internet, cyber security risks like man-in-the-middle assaults, sniffers, and denial-of-service attacks are serious problems. Data privacy is largely governed by law. Industry legislation in some nations prohibits offsite data storage, collecting, or disclosure for commercial use, such as the USA's Federal Information Security Management Act 2002, Canada's Personal Information and Electronic Documents Act, and the UK's General Data Protection Regulation [9].
- Standardize Communications: While data transfer occurs in IoT nodes and devices via Bluetooth, Wireless, ZWave, or even BigZee, cloud devices interact over TCP/IP Protocol using IP addressing.
- Location of data processing: Analyzing data obtained near the device node can frequently be the difference between averting catastrophe or cascading failures. Rugged IoT devices are necessary because fog nodes, which gather data from IoT devices, are typically dispersed over a wide geographic area with a variety of extreme weather conditions.

Over the Internet, cloud computing providers offer hosted, scalable enterprise applications. IoT is largely responsible for the rapid expansion of smart fog computing technology, which localizes physical computing, networking, and storage together with analytics and machine learning. To manage the fog data demand and delivery, cloud service providers such as Amazon, Google, Amazon, IBM, and Microsoft have enabled cloud-based delivery models for SaaS, PaaS,

CHAPTER 2

New Age Attacks on Smart Homes and Cyber-Physical Systems

Abstract: As smart homes and cyber-physical systems become increasingly integrated into our daily lives, they also become susceptible to new and sophisticated forms of cyberattacks. This chapter explores the emerging landscape of new age attacks targeting these interconnected environments. It delves into the diverse range of threats that exploit vulnerabilities in smart home devices and their underlying cyber-physical components. Through comprehensive analysis and case studies, this chapter sheds light on the potential consequences of such attacks and emphasizes the importance of proactive measures to safeguard these systems. By understanding these evolving threats, researchers, practitioners, and policymakers can collectively work toward fortifying the security and resilience of smart homes and cyber-physical systems.

Keywords: Cybersecurity, Cyber-physical systems, New Age attacks, Smart homes, Threat landscape.

INTRODUCTION

The proliferation of smart homes and the rapid evolution of cyber-physical systems have ushered in a new era of convenience, efficiency, and connectivity. These interconnected environments, collectively known as the Internet of Things (IoT) [1], have become integral to modern living, offering seamless control over devices and services. However, this heightened interconnectivity has also introduced unprecedented challenges in terms of cybersecurity. Traditional attack vectors are being eclipsed by a wave of innovative and highly sophisticated threats, often referred to as New Age attacks. The advent of smart homes and the rapid proliferation of interconnected cyber-physical systems have heralded a transformative shift in the way we interact with our environment. These innovative ecosystems seamlessly integrate everyday devices, appliances, and services, fostering convenience, efficiency, and enhanced quality of life. However, as these systems grow more sophisticated, they also become susceptible

Akashdeep Bhardwaj

to a new breed of cyberattacks that exploit the intricate interplay between the digital and physical realms. This chapter delves into the intriguing realm of New Age attacks, shedding light on their evolving nature and implications for smart homes and cyber-physical systems.

Cyber-Physical Systems or CPS [2] have emerged as powerful tools for addressing a wide array of challenges in interactions between devices and humans, particularly in scenarios where devices handle only a subset of solution parameters. This scenario is exemplified by air cooling split systems, which focus solely on room temperature and overlook factors like humidity, air renewal, filtration, and sanitization. Furthermore, traditional remote control-based adjustments for air cooling split systems fail to accommodate the dynamic complexities of real-world office environments. These complexities encompass fluctuating thermal loads due to factors like occupant count, equipment operation, external weather conditions, and individual preferences. Securing cyber-physical systems poses a formidable challenge, given their intricate composition encompassing diverse technological components, designers, operators, and users. Prior research has effectively illuminated the security complexities within such systems, highlighting the essential role of usable security in aiding humans to make effective security decisions and take appropriate actions. This book chapter centers its attention on the realm of intelligent cyber-physical systems, particularly those rooted in the IoT. These intelligent systems are designed to streamline and automate a multitude of functions, all while concealing the underlying complexity of end-users as illustrated in Fig. (**1**).

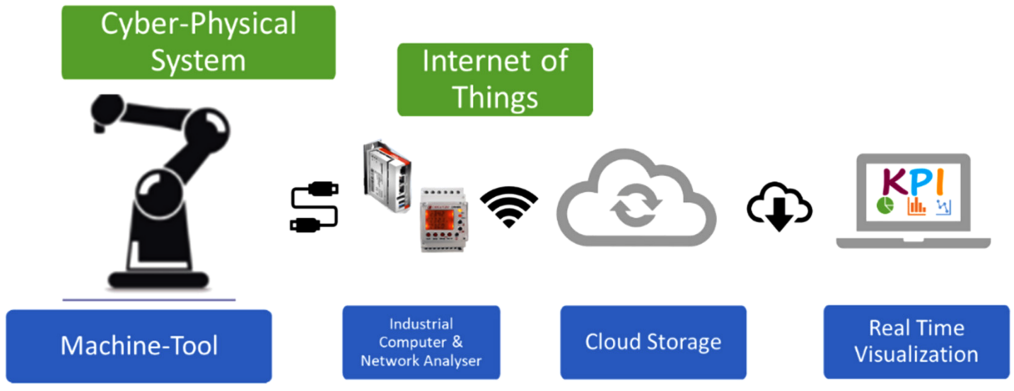

Fig. (1). Cyber-Physical Systems.

Cyber-physical systems encompass tangible systems or objects interwoven with computational capabilities and data storage functionalities. These CPSs rely on the interconnection of diverse sensor nodes, which communicate among

themselves and interface with components like actuators and microcontrollers, thereby orchestrating the behavior of the physical systems using intelligent algorithms. The seamless interaction between the physical and cyber domains hinges upon the efficacy of communication and networking algorithms, which facilitate this symbiotic relationship. IoT constitutes an integral facet of CPS, with sensor nodes forming interconnected networks where data is relayed through a multi-hop approach, ultimately reaching the root node. In the context of smart manufacturing, the Industry Internet of Things (IIoT) [3] and Industry Cyber-Physical System (ICPS) [4] have emerged as indispensable components. They cater to the pressing needs of modern industrial operations. The proliferation of intelligent sensors has ushered in an era of data explosion, yet this abundance poses multifaceted challenges within the real industry landscape. These challenges encompass the intricate task of constructing vast interconnected networks while ensuring data security and devising efficient access protocols. Moreover, the data's integrity is compromised by significant noise, a common occurrence in the context of industrial settings. Additional complexities involve adept data storage, seamless integration with cloud services, and the imperative for real-time analytics.

Traditional cyberattacks like viruses and data breaches have long been recognized threats, but the rise of New Age attacks presents a formidable challenge. These attacks leverage the convergence of technology domains to disrupt, manipulate, or compromise the functionality of smart homes and cyber-physical systems. Consider the example of a smart thermostat, a cornerstone of modern home automation. A New Age attack might involve manipulating the thermostat's settings remotely to compromise energy efficiency or even disrupt the heating system, leading to discomfort for occupants and potential property damage. Such attacks blur the lines between digital and physical impact, highlighting the need for a comprehensive security framework.

This chapter embarks on a comprehensive exploration of these emerging threats, focusing on their implications for smart homes and cyber-physical systems. While conventional attacks like malware and data breaches remain concerning, the evolving threat landscape encompasses novel approaches that exploit the intricate interplay between physical and digital realms. From supply chain vulnerabilities to AI-driven attacks, from cross-domain exploits to adversarial machine learning, this chapter aims to dissect these threats and illuminate their potential impact.

Through the lens of case studies and in-depth analysis, we will navigate the intricate web of vulnerabilities that New Age attacks target. By delving into real-world instances and conceptual frameworks, we seek to provide researchers, practitioners, and policymakers with a deeper understanding of the multifaceted

CHAPTER 3

Smart IoT and Machine Learning-Based Framework for Water Quality Assessment and Device Component Monitoring

Abstract: Water is the most important natural element present on earth for humans, yet the availability of pure water is becoming scarce and decreasing. An increase in population and a rise in temperatures are two major factors contributing to the water crisis worldwide. Desalinated, brackish water from the sea, lake, estuary, or underground aquifers is treated to maximize freshwater availability for human consumption. However, mismanagement of water storage, distribution, or quality leads to serious threats to human health and ecosystems. Sensors and embedded and smart devices in water plants require proactive monitoring for optimal performance. Traditional quality and device management requires huge investments in time, manual efforts, labor, and resources. This research presents an IoT-based real-time framework to perform water quality management, monitor, and alert for taking actions based on contamination and toxic parameter levels and device and application performance as the first part of the proposed work. Machine learning models analyze water quality trends and device monitoring and management architecture. The results display how the proposed method manages water monitoring and accesses water parameters more efficiently than other works.

Keywords: AI, Embedded, IoT, Microcontroller, Real time, Sensor, Wireless, Water quality monitoring.

INTRODUCTION

Just 2.5 percent or even less of the 71 percent of the water that coats the Earth's surface is safe for consumption. This results in serious effects in terms of elevated pollutant concentrations in freshwater sources as well as water shortages in various parts of the world. Freshwater supplies are depleting at an uncontrollable rate, and there is no other option for improving the situation than to track and sustain the highest possible level of water bodies. There have been many

Akashdeep Bhardwaj

developments in the 21st century, but there are difficulties in tracking water quality worldwide for clean drinking water in real time due to rising emissions and global warming. Water sources are dwindling, according to the Water Crisis Report, 2020 [1]. Deaths from the shortage of drinking water or water-related diseases are increasing, and over 850 million people worldwide have limited access to clean water [2].

In Africa, 19 million residents do not have access to clean water [3]. In India alone, waterborne diseases are expected to cost about $600 million per year. In India, less than 40% of the population has access to well-regulated drinking water. Water poisoning, mostly due to fluoride and arsenic, is found in 2 million homes [4]. Additionally, contaminants from old pipes or pollution can suddenly and unknowingly enter the water system, putting consumers at risk. In the United States, nearly 227 billion liters of treated water is lost each day due to leaking pipes [5]. Across England, every day nearly 3 billion liters [6] is lost due to old leakage water pipes, which is equivalent to almost 1200 Olympic swimming pools. Better methods for monitoring real-time water quality need to be established. Given the strong digital presence in everyday life, several service utilities gather data and track devices manually. This inefficient process leads to inaccurate and incomplete measurements of data and assets. When upgrading, utilities need to think about how to scale to thousands or even millions of sensors, water pumps, meters, and valves. With advances in IT infrastructure, water purification and desalination plants and systems can be integrated with IoT devices, sensors, and embedded systems to improve the storage, monitoring, and alerting for water quality and the devices involved. Using machine learning, systems and sensors can gather data and generate alarms in real time to detect problems and reduce the load on the infrastructure and staff who currently manage the processes. Traditional techniques to monitor water quality include a manual sampling of water samples from various sites. When handled correctly, the infrastructure update can unlock new insights and reach unprecedented levels of efficiency.

When evaluating how to start updating infrastructure with this technology, utilities should keep in mind a wide range of possibilities for IoT in water management. At the forefront, security should be a priority. A foreign attack on a community's system can cause irreparable damage. Processing data in an efficient manner involves installation and monitoring of water usage, leak detection, advanced metering, and water quality for real-time data and situational awareness. Highlights of this research are as follows:

- Smart devices monitor, manage and alert real-time water quality, contamination, and toxic parameters.
- Perform proactive monitoring and alerting of systems and devices involved.

- Machine learning models to analyze water quality trends and device management architecture.
- Random forest had robust results and achieved an accuracy of 88% with XGBoost of 0.85; even Naïve Bayes displayed the least accuracy of just 49%.

This research is organized in sections. Section II reviews smart water management solutions and Section III reviews previous research works and implementations. Section IV presents the proposed framework using IoT; Section V reviews the critical parameters to monitor and manage and Section VI presents a machine learning model to analyze water quality trends and device management architecture. Section VII presents the results obtained, and finally, the conclusion with the future scope is presented in Section VIII.

SMART SOLUTIONS FOR WATER MANAGEMENT

Smart sensor devices aid in efficient and safe water management for consumers and workers through real-time data collection, alerting, and actions to prevent issues from occurring. Depending on the infrastructure, numerous processes can be automated, real-time alert generation, and insights gathered for attaining high-efficiency levels. Water industrial infrastructure having such devices and sensors aids in delivering several benefits to utilities and their teams when it comes to maintaining physical infrastructure and ensuring the safety of utility workers. With the influx of data, service teams manage remote infrastructure and reduce physical maintenance on site. Service teams are alerted when any part of the infrastructure is at risk, even as automated processes perform the necessary changes proactively instead of sending service teams onsite to address the issues.

Water Processing, Storage, and Distribution

Water distribution affects the economic growth of every country; however, water loss due to leakage is prone to contamination. This affects people's health and welfare. According to a study released by the World Health Organization, about 2.2 billion global population does not have accessibility to drinking water. There is a need to ensure water safety and waste reduction by using IoT. There are several conventional techniques for collecting water datasets such as hydrologic storage like moisture, streamflow, recharge, ocean-land-atmosphere fluxes, water-land-air quality measures, and energy demand to quantify their accuracy, but handling and tracking the data in real time is difficult due to the heterogeneity of the data, the time it takes to obtain it, the resources needed for transmission, and the network's coverage and accessibility. With new-age technology, tracking water quality [7] in real time to receive alerts and perform proactive corrective actions becomes possible.

CHAPTER 4

Smart Water Management Framework for Irrigation

Abstract: The demand for and pressure on natural resources worldwide is rising, placing more emphasis on the availability of clean, safe drinking water. Modern technologies like cloud computing, embedded systems, and smart sensors can provide safe and effective control of the supply of drinking water for agriculture and consumer usage. By combining proactive alerting, monitoring, and real-time data collection with proactive management measures, problems are avoided before they arise. This study offers a clever and safe foundation for future research aimed at improving the current irrigation system. This is a low-cost irrigation strategy that uses smart device sensors and cloud connectivity to give automated management and needs according to the environment and season. In order to address the operational failures, this also provides alerting scenarios for device and component failures as well as water leaks by immediately switching to an alternate mode and delivering alert messages about the problems.

Keywords: Cloud computing, IoT, Internet of Things, Smart irrigation, Smart farming.

INTRODUCTION

Disruptive advancements in technology have permeated business settings, greatly improving people's quality of life. The foundation of the fourth Industrial Revolution is the Internet of Things and smart gadgets, which have enormous potential for automation and decision-making in the conventional agricultural and industrial sectors. These devices also have intelligence built in and can adapt intuitively. With the use of smart devices and sensors, cloud computing, big data processing online, and artificial intelligence characteristics, the Internet of Things (IoT) offers the technological capacity to run and manage industrial infrastructure automatically and more efficiently. Drinking water will be scarce in more than 50% of metropolitan places worldwide by 2025, even though water is the most

Akashdeep Bhardwaj

valuable resource. To prevent this kind of situation and identify impending water shortages, smart water management must be put into practice immediately.

Legacy SCADA (Supervisory Control and Data Acquisition) models operate most of the world's water facilities today. Because of their practical constraints, these industrial units are inefficient and mainly incapable of monitoring, detecting, or operating water distribution. According to UN Scarcity (UN Scarcity, decade, 2020) [1], by 2025, there will be a water deficit on every continent, with over 1.2 billion people—roughly one-fifth of the world's population—forced to live in water-scarce locations. One-fourth of the world's population, or 1.6 billion people, do not have access to intelligent water management systems that can handle salty water from rivers and subsurface resources. An estimated 6 billion gallons of treated water are lost yearly in the US alone due to leaky water pipes and ineffective distribution.

Consumers are also in danger from the monitoring of pollutants and toxins that enter the water pipelines after treatment. Sensor-based solutions for smart water management provide effective and efficient operations with no need for human involvement. By using IoT sensors and linked field nodes, which enable immediate reaction based on current weather and landscape conditions, remote monitoring and smart water management may help optimize water consumption and remove the difficulties associated with resolving issues with distant irrigation systems. The optimization of resource usage and component monitoring are the main advantages of implementing smart water management in water plants. Smart water management offers the greatest implementation choices, from detecting leaks and water waste to matching water supply demands with component and device up-times.

Energy conservation and efficient pumping are essential to guaranteeing a steady supply of water for future generations, whether it is treated or potable. One major burden for utilities is the increasing cost of electricity due to inefficient water pumping. It may represent as much as 30% of total operational costs. When infrastructure is upgraded, utility firms may utilize IoT to improve the efficiency of water management and increase worker and customer safety. The effort of staff members who oversee physically examining every square inch of infrastructure may be lessened by using these smart devices and sensors to help with real-time data collection and alerts. When determining how to start implementing IoT in water management to modernize infrastructure, utility firms should consider a wide range of choices. Security needs to be first on the list of priorities. An infrastructure strike by a foreign power might have disastrous effects. To gather real-time data and enhance situational awareness, it will also be essential to analyze data quickly. This starts with the installation of monitoring systems for

water usage (Advanced Metering Infrastructure), leak detection, and water quality. Scalability and management of the system should also be considered.

The fact that a lot of utilities still manually track devices and data may surprise you, considering how much digital technology is used in our daily lives. Data and asset measurements that are out-of-date, inaccurate, or incomplete might be produced using this outdated and ineffective technique. When upgrading, utilities must think about how to extend to hundreds, or perhaps millions, of sensors, water meters, and valves. The infrastructure improvement achieves previously unheard-of levels of efficiency and yields fresh insights. If different corporate, social, and technological considerations are taken into consideration, it is conceivable to give Internet of Things capabilities in water management scenarios. The main benefits of utilizing IoT in water management are higher efficiency and cost savings since real-time operational control enables water management companies to make wiser decisions.

By leveraging real-time data from sensors and actuators, these smart devices monitor and improve water management systems, increasing their efficiency and reducing energy costs. Lowering water management costs is possible with increased production, methods, and appropriate use. Better service and more usage might be advantageous to businesses and consumers alike. By using sensors and connectivity to improve asset tracking (devices, machines, tools, and equipment), businesses may gain information about their supply chains and assets. They can promptly recognize assets and carry out routine maintenance on important machinery and infrastructure. Any firm that wants to succeed must be productive. Completing activities using sensor and IoT devices is facilitated by real-time data collection, improved component and resource control, process and service optimization, time and capacity reduction, and optimization. In turn, this is narrowing the skill gap between needed and available, increasing labor efficiency.

The aim of this study is to explore IoT water management systems that utilize algorithms for irrigation farming and to uncover innovative technologies that enhance farming efficiency and effectiveness.

LITERATURE REVIEW

Three hundred and seventy published studies were found by the author in peer-reviewed publications such as IEEE, ACM, CMC, Elsevier, and Springer. To identify and choose the articles for this research, the authors grouped and condensed the papers based on research on smart water management, IoT, embedded sensors, devices, and cloud computing. The literature reviews are categorized according to the chosen keywords for this research in Table **1**, and the

CHAPTER 5

Secure Framework against Cyberattacks on Cyber-Physical Robotic Systems

Abstract: Robot-based platforms and processes have integrated the security and efficiency of data into a comprehensive range of domains like manufacturing, industrial, logistical, agricultural, healthcare, and Internet services. Smart cyberattacks have been on the rise, specifically targeting corporate and industrial robotic systems. These attacks are executed once the IoT, Internet, and organization integration is implemented with the industrial units. The authors implemented security criteria-based indices for Cyber-Physical systems (CPS) with industrial components and embedded sensors that process the information logs and processes. The authors proposed an attack tree-based secure framework that does not include every CPS device; however, it takes into consideration the critical exploitable vulnerabilities to execute the attacks. The authors categorized each physical device and integrated sensors based on logs and information in a sensor indices device library. This research simulated the real-time exploitation of vulnerabilities in CPS robotic systems using the proposed framework in the form of a two-phased process. This validates the enhanced data security output of the integrated sensor and physical nodes with the intelligent monitor and controller system health monitor during real-time cyberattacks. This research simulated common cyberattacks on cyber-physical controller servers based on cross-site scripting and telnet pivoting. The authors gathered known and unknown vulnerabilities and exploited them with a tree-based attack algorithm. The authors calculated the average time for cyberattackers with different skills when trying to compromise CPS devices and systems.

Keywords: Attack framework, Cyber-physical, Robotic security, Robotic platforms, Telnet pivot, XSS.

INTRODUCTION

Given the extent to which digital technologies and physical devices have infiltrated our lives, there is a belief that this closer integration with many other disciplines will only grow to new heights in the near future. The new age of Industrial Revolution 4.0 is largely concerned with future systems of digital

Akashdeep Bhardwaj

manufacturing. In homes, smart sound, light and heating solutions, housekeeping robots, and air conditioning systems connect and integrate with computational systems and devices. The transportation domain includes cars, planes, and electric bicycles. Healthcare pacemakers, personal assistance robots, insulin pumps, and smart prosthetics provide immense help to patients. These technologies did not exist until recently, yet now they offer the potential to save and improve the quality of life tremendously. Wearable fitness and health monitoring devices offer the potential for a huge positive impact on healthy people as well as those with physical or cognitive disabilities. Industry monitoring and control systems involve the use of sensors and networks to observe large land or marine areas. Examples from the energy sector include smart grids, windmills, and technologies to harvest green energy. It is no exaggeration to imagine the entire planet Earth as a massive cyber-physical ecosystem. However, highly sophisticated problems and hazards arise from hostile threats and Internet attacks, which include robotic platform malware, hijacks, and remote control.

Smart industrial production systems generate goods using computer-integrated processes, networks for intelligence, cybernetics, and mechatronics (Robotics and Cyber-Physical Systems, 2019) [1]. CPS integrates physical dynamics, monitoring, and control servers with software application components and networks. This smart production system incorporates real-world physical and computer components, which result in highly monitored and controlled states and parameters for optimum production. These are entwined to operate at temporal and spatial states to monitor and control physical processes and vice versa. Smart grids, industrial control units, driverless cars, automatic pilot avionics, autonomous automobiles, and robotic systems [2] are some common examples of CPS. CPS shares a relatively similar architecture to the Internet of Things (IoT) but does not work in a standalone manner. CPS operates in an automated manner with a higher level of coordination and processes as an interacting combination of computational components and physical devices such as actuators, robots, embedded sensors, and human machine interfaces in production facilities. Such infrastructures provide technical solutions and promote new efficient human engagement with various domain architecture and abstractions, such as consumer, energy, infrastructure, environmental, healthcare, manufacturing, military, physical security, smart cities, transportation, and robotic equipment and machinery.

To maximize the use of resources and system performance, CPS combines and collaborates computing and physical processes connected to the Internet or an internal secure data center. However, cyber threats and attacks through internal networks or internet access jeopardize the security of physical and computational interacting elements. These smart cybersecurity attacks infiltrate CPS *via* the

cyber or the networked component to attack the primary controllers, industrial servers, computers, PLCs, and robotic systems. Secure connection to external networks has always been a security concern for CPS deployments. CPS controllers suffer irreparable damage when attackers discover new ways to access the control systems to alter their services and configurations. Although cyber mitigation systems such as end-point security, anti-virus shields, or network intrusion detection devices have emerged as possible solutions for internal attacks, smart cyberattacks and threats have been multiplying and getting sophisticated. CPS suffers badly in this regard, as control and security are solely served by the command-and-control server and the devices are often secured by no other protection. Smart security attacks on the cyber layer to the CPS systems have an intrinsic causal impact. More recent cyberattacks include the Colonial Pipeline attack [3] in May 2021, which suffered a ransomware attack that affected the computer systems and equipment managing the pipeline. Company operations were halted as the Colonial Pipeline ransomware attack cost 75 bitcoin or US $ 4.4 million. Stuxnet [4] and Aurora [5] attacks raised the need to recognize the high-priority requirement of protection of critical physical infrastructures.

In this context, CPS is a fresh field for research for designing and deploying mitigation measures to counter and mitigate smart cyberattacks. Interest in the security of industrial infrastructure has increased for collaborative robotic systems working on vital infrastructures with automatic and semi-automatic assembly processes globally. In recent times, attention to managing and mitigating cyber risks by reducing security gaps posed by automation processes or manual actions has gained huge consideration. Cyber safety and detection solutions are designed for cyber-physical systems running on collaborative-networked ecosystems.

Highlights of this research include:

- Unique taxonomy of cybersecurity attacks on cyber-physical systems: The novel aspect of this classification is to identify smart cybersecurity-related issues for robotic industrial CPS applications. Research papers and vendor vulnerabilities are categorized based on cyberattack causes, attacks, threat vectors, threats, and risks involved.
- Secure framework to enable safe and secure human-robotic system collaboration in industrial environments: The proposed secure CPS framework can help reduce threats such as information breaches, data transfers, or alternations in device logs from smart cyberattacks on the computational nodes, devices, and interfaces connecting various physical components.
- Algorithms for determining the anomalies in the sensor logs due to smart cyberattacks.
- Detect DoS attacks by focusing on the anomaly values due to denial-of-service

CHAPTER 6

Multinomial Naïve Bayesian Classifier Framework for Systematic Analysis of Smart IoT Devices

Abstract: Machine learning and artificial intelligence-based sentiment analysis are crucial for companies to automatically predict whether the customers are happy with their products. In this paper, a deep learning model is built to analyze thousands of reviews of Amazon Alexa to predict customer sentiment. The proposed model can be directly applied to any company that has an online presence to automatically detect customer sentiment from their reviews. The objective of this research work is to propose a suitable method for analyzing the users' reviews of Amazon Echo and categorizing them into positive or negative reviews. In this research work, a dataset containing reviews of 3150 users has been used. Initially, a word cloud of positive and negative reviews has been plotted that gave a lot of insight from the text data. After that, a deep learning model using a multinomial naïve Bayesian classifier has been built and trained by using 80% of the dataset, and then the remaining 20% of the dataset has been used for testing the model. The proposed model gives 93% accuracy. The proposed model has also been compared with four models used in the same domain, and it outperformed three of them.

Keywords: Artificial intelligence, Alexa, Amazon, Deep learning, Internet of Things, Machine learning, Natural language processing, Smart devices.

INTRODUCTION

In recent years, intelligent voice assistants like Microsoft's Cortana, Apple's Siri, Amazon's Alexa, and Google's Assistant have become very popular and used widely in the day to day life. These intelligent voice assistants have changed the way users interact with smartphones or computers. Individuals are using these intelligent voice assistants to give voice commands and get the appropriate information like daily news, weather reports, or fulfillment of commands like playing media. Along with these uses, voice assistants are also used to perform some basic tasks like setting timers or alarms and making phone calls. Nowadays, these voice assistants, especially Alexa, are also used in smart IoT-enabled

Akashdeep Bhardwaj

devices to support voice control. The voice assistants are connected to the internet. Whenever a user gives any voice command, then that command is sent to a central computing system for analysis. In the central computing system, the command is analyzed and translated by the voice assistants using natural language processing (NLP), and a proper response for that command is provided by the voice assistant. Recent advances in NLP have allowed voice assistants to generate meaningful responses rapidly [1].

With the help of artificial intelligence (AI), intelligent voice assistants can also be used to detect or understand the emotions of the user and perform sentiment analysis. Sentiment analysis plays an important role when users choose to share their feedback or experience regarding some product through voice assistants. By using sentiment analysis of voice assistants, commercial business companies can use insights to improve their products or services. It is very important for the voice assistant to accurately detect the sentiment in the users' feedback or product review and analyze it to detect the correct tone and mood of the user. With the help of AI and NLP [2], the magnitude of the mood and tone of a user can be calculated, and a numerical score can be assigned to them. Depending on the outcome of the sentiment analysis, proper assistance can be provided to the user. As the popularity of intelligent voice assistants is increasing, the number of services supported is also increasing very rapidly. After using a product, most users like to share their experience about the product by writing reviews. This review not only helps the potential buyers but also helps the business companies in making good, impactful decisions about the product. So, it is very important to perform sentiment analysis on users' reviews about the product and the services provided by that product. The product reviews are mostly available in text format. AI-based sentiment analysis [3] can be used to classify the products' reviews into positive or negative categories by looking at the words used in the review. Generally, a positive product review contains words like good, easy, love, happy, and great, and a negative review contains words like disappointing, difficult, frustrating, bad, waste, not, and annoy.

In this research work, the authors have predicted customer sentiment from real Amazon Echo customer reviews by using NLP. The main objective of this research work is to predict whether the users are happy or not with the Amazon Echo. If the customers are not happy with the product, then Amazon can figure out the reason and can help the users with proper assistance and/or update the product based on the reviews. In this research, a deep learning model has been built and trained to analyze thousands of reviews of Amazon Echo to predict customer sentiments.

The remainder of this work is organized as follows: the Related Work section highlights the relevant work done in the same area; the Research Methodology section describes the step-by-step implementation of the method used in this research; the Results and Comparison section describes the results and compares them with the similar models in the same domain; Conclusion section conclude the research.

RELATED WORK

The authors researched 354 journal publications since 2018 from IEEE, Springer, MDPI, ACM, Elsevier, and other highly referred journals. Based on the research reviews, keywords, and results, the papers were classified to match the relevant work and results of this research. The authors shortlisted research that is relevant as per the below selection methodology to finalize 35 research articles, as illustrated in Fig. (**1**).

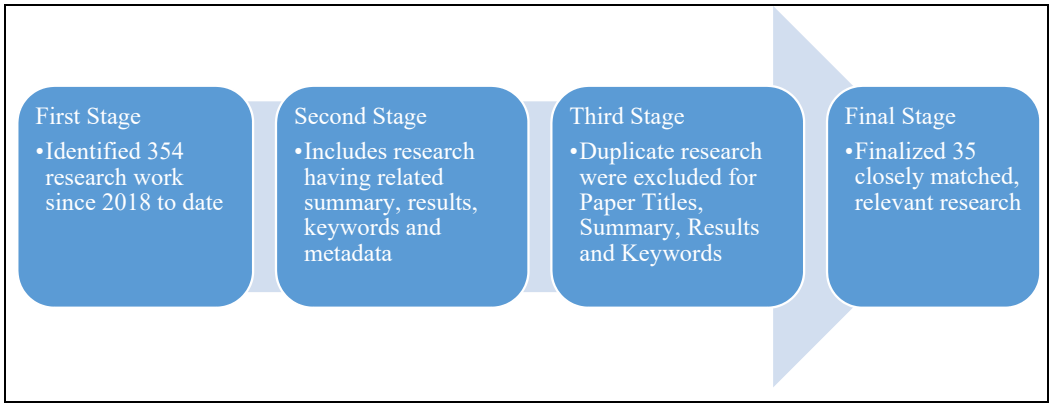

Fig. (1). Research selection methodology.

The final 35 research studies selected were categorized as illustrated in Table **1** for works closely matching the metadata, summary, and keywords deep learning, artificial intelligence, voice assistant, and IoT devices, among others. The classification provided an overall distribution ratio between 17 to 24 percent.

Table 1. Research selection and classification.

Grading Classification	Stage 1	Stage 2	Stage 3	Stage 4	Breakup
Deep Learning	71	45	18	7	**20.06%**
Artificial Intelligence	82	52	20	8	**23.16%**
Alexa	69	44	17	7	**19.49%**
Voice Assistant	63	40	16	6	**17.80%**

CHAPTER 7

IIoT: Traffic Data Flow Analysis and Modeling Experiment for Smart IoT Devices

Abstract: The Internet of Things (IoT) has redefined several aspects of our daily lives, including automation and control of the living environment, innovative healthcare services, and much more. Digital IoT devices and sensors, when integrated with home appliances, industrial systems, and online services in the physical world, have brought intense, disruptive changes in our lives. The industry and home users have widely embraced Internet of things or IoT. However, the innate, intrinsic repercussions regarding security and data privacy are not evaluated. Security applies to Industrial IoT (IIoT), which is in its infancy stage. Techniques from security and privacy research promise to address broad security goals, but attacks continue to emerge in industrial devices. This research explores the vulnerabilities of IIoT ecosystems not just as individual nodes but as the integrated infrastructure of digital and physical systems interacting with the domains. The authors propose a unique threat model framework to analyze the attacks on IIoT application environments. The authors identified sensitive data flows inside the IIoT devices to determine privacy risks at the application level and explored the device exchanges at the physical level. Both these risks lead to insecure ecosystems. The authors also performed a security analysis of physical domains and digital domains.

Keywords: IoT security, Data privacy, Sensitive data, IIoT apps, Physical device, IIoT threat model.

INTRODUCTION

IoT has flourished in every area possible, be it industry, agriculture, energy projects, or transportation. Its plays a major role in transforming the analog world into a digital one. Industrial IoT tops the list in the applications area. The industrial IoT application field encompasses various linked “things” or initiatives within and outside factories and manufacturing facilities. Many IoT-based factory control and automation initiatives, for example, offer holistic innovative factory technologies with multiple features such as manufacturing department monitoring,

Akashdeep Bhardwaj

wearables, augmented reality on the production floor, remote programmable logic control (PLC), or computerized quality management systems. An IoT system comprises sensors and devices communicating with the cloud over the Internet connection. Once the data reaches the cloud, software analyzes it and may decide to act, such as sending an alarm or automatically altering the sensors/devices without the need for the user's intervention. A user interface allows users to enter information or check in on the system if required. Any changes or actions taken by the user are then communicated back in another manner *via* the system: from the user interface to the cloud and then back to the sensors/devices to effect change.

A smart factory is a computerized manufacturing facility that collects and shares data continually through linked devices, machines, and production systems. This information is then utilized to judge how to enhance procedures and deal with problems. Connectivity, data analysis, and diagnostics are important ideas underpinning the future factory, resulting in fewer shutdowns, enhanced processes, and optimized facilities. A smart factory makes use of cutting-edge technology and networking to optimize processes. IoT and artificial intelligence are more responsive and also predictive in using available resources to produce cost-effective and efficient manufacturing. Assessing the manufacturing chain aids in selecting components and assessing these key regions, which may reveal what should be improved next. This investigation should be led by a varied team of professionals with expertise in many business areas. IoT engineers collaborate with management and IT system professionals to identify areas for improvement and optimize operations, boost sales, lower costs, and save time throughout the production process. Apart from industry, IoT is revolutionizing with an unstoppable speed in every area possible, such as transportation/mobility, healthcare, supply chains, and cities. The IoT was only a notion in the early 2000s; as we approached 2021, indications indicated that this innovation was here to stay. According to reports, 35.82 billion IoT devices would be deployed globally by 2021 and 75.44 billion by 2025 [1]. From homes, healthcare, and electronics to industrial, mechanical, and manufacturing for monitoring, alerting, and automation, IoT devices running application services have transformed human-digital interaction in the lives of home users and the industry. The contact between students and teachers and between students throughout the learning process can occur in synchronous and asynchronous forms, as well as face-to-face and electronic modes. Interaction with a smartphone app, visiting a website from a computer, and using IoT devices are all instances of human-computer interaction.

Although home users and the industry have embraced the systems supporting IoT, the security and privacy implications of these devices on our lives are still not

fully understood. IoT installations have access to application functionality that, if exploited, might jeopardize user security. These IoT systems have complete access to sensitive private information, which, if released, might result in privacy concerns. As a result, it is necessary to identify potential hazards to any digital device before deploying it and include suitable protections in the system as it is developed and architected. Understanding how an adversary might be able to identify common ground with a system helps guarantee that proper mitigation mechanisms are in place from the start. Thus, building the product with security in mind from the start is vital. In linked corporate IoT devices, their manner of conceivable contact surface areas and communication patterns must be studied to create a framework for safeguarding internet access to those gadgets. The term 'digital access' is used to distinguish actions carried out with direct device connection from those carried out with physical access control's access security. Place the gadget in a room with a locked door, for example.

Physical access cannot be prevented by software or hardware. However, efforts may be made to avoid physical access from communicating with the device. Evaluating the security of IIoT-based smart settings such as commercial and smart homes has become critical to effectively reducing security threats and dangers associated with deploying smart IIoT-based electronics devices. Since IIoT applications are exposed to a large amount of sensitive data from various sensors and devices connected to the central, one of the main criticisms of concurrent systems is that current commercial methodologies lack basic tools and services to analyze what they do with that data, pointing to application privacy. There are few tools available for assessing privacy threats in IIoT applications. The need is a set of analytic tools and methodologies aimed at platforms that may detect privacy problems in IIoT apps. This study investigates the methodologies and tools for defining the use of critical material and identifying vulnerable data flows in IoT deployments.

Conventional sensitive data tracking solutions built for mobile apps and other areas are insufficient. Existing tools may overlook sources such as sensor status (locked/unlocked) and media such as IIoT network connections, making them easily evaded by rogue programs. Second, security-critical design defects in the permission architecture of IoT platforms, such as over-privileged device controls caused by present coarse-grained access restrictions, necessitate analysis sensitive to these privileges and their impacts. Finally, IoT-specific technologies such as system parameters and web application IIoT apps differ greatly from other platforms; hence, on-demand algorithms are necessary to ensure accuracy. Symmetric encryption techniques employ a single cryptographic key to encrypt and decode the data received. The technique is relatively simple because just one key is utilized for both actions. The main benefit of symmetric encryption is this.

CHAPTER 8

Comparison of IoT Communication Protocols Using Anomaly Detection with Security Assessments of Smart Devices

Abstract: The authors implemented an attack scenario simulating attacks to compromise node and sensor data. This research proposes a framework with algorithms that generate automated malicious commands, which conform to device protocol standards and bypass compromise detection. The authors performed attack detection testing with three different home setup simulations and referred to accuracy of detection, ease of precision, and attack recall, with F1-score as the parameters. The results obtained for anomaly detection of IoT logs and messages used K-nearest neighbor, multi-layer perceptron, logistic regression, random forest, and linear support vector classifier models. The attack results presented false-positive responses with and without the proposed framework and false-negative responses for different models. This research calculated precision, accuracy, F1-score, and recall as attack detection performance models. Finally, the authors evaluated the performance of the proposed IoT communication protocol attack framework by evaluating a range of anomalies and compared them with the maliciously generated log messages. IoT Home #1 in which the model involved IP Camera and NAS device traffic displayed 97.7% Accuracy, 96.54% Precision, 97.29% Recall, and 96.88% F-1 Score. This demonstrated the model classified the Home #1 dataset consistently.

Keywords: Cyberattacks, Internet of Things, IoT, IoT attacks, IoT communication, IoT framework, IoT protocols.

INTRODUCTION

The use of smart home and industrial devices for gathering and processing data has increased significantly in the past few years, including user comfort levels and task automation. Such devices on the Internet or IoT do not include high-end security features, as the hardware components deployed in IoT devices lack security assurance, integrity, and privacy. This paper compared datagram and transport layer security protocol versions for IoT devices. IoT is one of the

Akashdeep Bhardwaj

fastest-developing domains, estimated to reach about 1.4 billion devices by 2023 [1]. IoT is the future phase of communication, with physical devices being able to generate, receive, and exchange data seamlessly. IoT applications aim to automate various operations and enable passive physical things to operate without the need for humans. IoT is a complex technology, which is an extension of the current Internet, blending digital technology into our physical world. IoT devices communicate with other nodes and sensors based on the changes in the environment and send that data to other IoT nodes. The devices are segmented into B2C or business–to-consumer, including the end-user or customers, and business-tobusiness. The IoT ecosystem is built upon the hardware-defined sensors, integrated circuits, and microcontroller components that collect data andsend it to the software. It defines modules that transform it into useful information and send this transport network layer for analytics to provide value and intelligence.

These low-quality devices do not implement any advanced data encryption or device authentication. This leads to the failure to mitigate threats posed by attacks on these devices and ecosystems. Due to the nature of the Internet, attackers deploy command-and-control servers to sniff and inject malware to compromise IoT node-to-node communications. Recently, IoT devices have increased the embedded system's network connectivity and computing capability. The large-scale deployment of IoT has affected our lives significantly. This displays the lack of protection and security protocols on the IoT software and hardware side, which are marked as entry points for attackers to launch malicious attacks. These devices are implemented as smart sensors that can share information about their environment, *e.g.*, wearable health monitors, wireless inventory trackers, and as connected devices that send data to the Internet about that device's state or receive commands to execute actions and take subsequent steps. This ability of IoT devices to ‘talk’ to other devices and move the generated data at the edge points to the central servers makes them valuable. This interaction happens using multiple IoT communication protocols, which, as an integral collection, are essential to ensure the IoT ecosystem works. Yet, these IoT protocols do not work efficiently in every scenario. Each protocol has different features and combinations of capabilities, making them suitable for specific IoT deployments. These deployment features depend on power consumption, speed, battery life, physical barriers, device cost, and the geographical environment. The communication is built upon the network technology stack for data to be transferred across the entire ecosystem. However, due to a lack of security, IoT communication protocols are insecure. Due to a lack of security, an attacker might launch an attack and leak sensitive data, potentially exposing the entire network. The gadgets are always linked and in constant communication, both within and outside the network. IoT device-to-device interactions allow these things on the Internet to communicate

with one another to transmit data, receive and send orders, and communicate in general. The major IoT protocols are illustrated in Fig. (**1**) and described below:

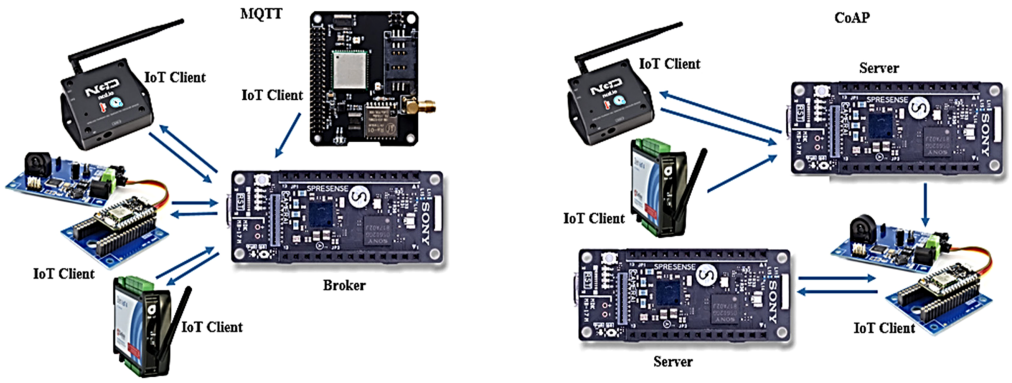

Fig. (1). IoT Communication protocols – MQTT & CoAP.

- MQTT, or the Message Queuing Telemetry Transport protocol, works using publish-subscribe architecture. This enables one too many communications and is mediated by a controller or broker node. The messages are sent, received, and categorized by topics, which function as labels. The protocol can work unreliable, with unpredictable high latency and low bandwidth.
- CoAP or Constrained application protocol [2] works with HTTP over UDS for secure communications; this allows devices to work in environments having low energy, availability, and bandwidth [3].
- MPQ or Advanced message queuing protocol [4] allows interoperability between different IoT nodes irrespective of the platforms or the message brokers. This offers reliability and security.
- BLE or Bluetooth using short wave, ultra-high frequency radio communication (How to Deploy Cassia Bluetooth) [5] for audio data streaming during short distances. This IoT protocol tends to consume less power than the standard Bluetooth connections, so it has become appealing for wearable devices deployed in healthcare, trackers, or fitness consumer and commercial products.
- LoRA or Long Range [6] is a non-cellular wireless protocol for secure data transmission.

Although IoT technology is still evolving, IoT attacks have already matured. The research community has recently focused on security challenges affecting the Internet of Things platform. The popularity of low-cost, short-range data transmission is primarily due to the recent explosion of IoT devices combined with the requirement for an economical way of transmitting data. Since no single IoT protocol is best suited for every deployment, IoT design architects must

CHAPTER 9

All-Inclusive Attack Taxonomy and IoT Security Framework

Abstract: In the early 2000s, the Internet meant being able to connect different communication devices, whereas the focus in the last few years has been on connecting 'things' to the Internet. Although there is no distinct classification for these devices and things on the Internet, the Internet of Things (IoT) ecosystem primarily consists of a complex network of devices, sensors, and things. These 'things' are controlled by humans and utilize the existing cloud infrastructure. These devices provide facilities and benefits to make our lives comfortable. IoT domains include smart homes, healthcare, manufacturing, smart wearables, smart cities, smart grids, industrial IoT, connected vehicles, and smart retail. Different IoT models involve human-to-IoT, IoT-to-IoT, and IoT-to-traditional system architectures. In most scenarios, the architecture ends up connecting to the unsecured Internet. This has thrown open several critical issues leading to cybersecurity attacks on IoT devices. IoT communications, protocols, or architecture have never been conceptualized to handle the new age of cybersecurity attacks. IoT devices have limited computing, storage, networks, and memory. In this research, the authors present a unique IoT attack framework named IAF, focusing on the impact of IoT attacks on IoT applications and service levels. The authors also propose an all-inclusive attack taxonomy classifying various attacks on IoT ecosystems.

Keywords: Attacks, Framework, Internet of Things, Layers, Security, Taxonomy.

INTRODUCTION

The Internet of Things (IoT) ecosystem involves interconnected IoT devices in complex architectures. The IoT has been increasing at a significant rate in the past few years. IoT security needs to be assigned the highest priority while developing, configuring, or updating against cybersecurity attacks. This ensures optimal performance throughout the deployment with authorized user access. IoT security [1] has been a work in progress, presenting attractive, low-hanging targets for cyber-attackers. Easy accessibility and vulnerabilities in devices and components, and more importantly, the quality of data gathered by those sensors are the main

Akashdeep Bhardwaj

reasons for the rise in cyberattacks against smart devices and IoT deployments. Vulnerable IoT devices connected to the command center, as well as other devices, present high risk to every device and system on the same network. Such attacks can lead to huge losses and damage [2]. IoT deployment designs and distributed nature, along with limited computation capability, network, and storage capabilities, certainly make them exploitable targets. IoT sensors and actuators are tempered effortlessly and are even susceptible to physical attacks. Implementing software security is also not sufficient to secure such devices. IoT attacks on such distributed ecosystems are not just confined to the applications or network layers. There is a huge demand for implementation security [3] for the hardware components and at firmware levels. Therefore, the logical and physical security of these devices should be paramount, regardless of their count or cost.

Advancements in various domains, along with disruptive technologies, have led to the development of many innovative devices. IoT [4] involves people, devices, and various ‘things' connected on the Internet. These ‘things’ are accessed at any time and at any place. IoT technology focuses on creating a better world with objects around humans. These objects or things are supposed to know what we want and when to process our demands. The IoT ecosystem consists of many smart devices interconnected [5] with each other in complex networks. These are heterogeneous and either use wired or wireless ports. When billions of IoT devices are connected, the ecosystems turn into the Social Internet of Things or SIoT, when such devices share data and social sites. This leads to security and privacy issues. The solution is to have secure communication from IoT devices to IoT applications with end-to-end encryption. IoT architecture designs are layered deployments, which comprise the spplication layer, which includes cloud infrastructure; the transportation layer, which includes networks; and the preparation layer, which consists of sensor components and devices.

LITERATURE SURVEY

Contributions of different papers about the current issues are shown in Table **1**.

Table 1. Literature Survey on IoT Attacks.

Reference	Relevant Keywords
Reddy *et al.* (2019) [6]	Internet of Things, IoT Networks, Telecommunication Security, Trusted Computing, Collusion Attacks, Trust Computation, Trust Model, Mitigate Badmouthing attacks, Malicious object, Similarity model, Computational modeling, Reliability, Sensors, Security, Cloud, Data models, Trust, Recommendations, Similarity, Privacy.

(Table 1) cont.....

Reference	Relevant Keywords
Vishwakarma *et al* (2019) [7]	IoT Protocols, Computer Network Security, Internet of Things, Invasive Software, Learning (Artificial Intelligence), Detection Framework, IoT Botnet, DDoS attacks, IoT Security, IoT Malware, Zero-day DDoS, Machine Learning, Malware Detection, Honeypot-based Approach, Computer crime, IoT honeypot, Data models.
Luo *et al.* (2019) [8]	Network Security, Distributed Denial of Service Attacks, Internet of Things, DDoS Attacks, SDN, Invasive Software, Software Defined Networking, IoT devices, Moving Target Defense Architecture, Malware, Network Asset, Computer Crime, IP Networks, Malware, Botnet, SDN, Honeypot, DDoS Attack, IoT Security
Shah *et al.* (2018) [9]	Internet of Things, IoT Protocols, IoT Security, Secure IoT Systems, IoT Server, IoT Device, Network Security, Message Authentication, Authorization, Public Key Cryptography, Single password, Secure Vault Change, Dictionary Attacks, Side-channel Attacks, Multi-key-based Mutual Authentication, Multi-password-based Mutual Authentication, Arduino, Authentication, Encryption.
Kepçeoğlu *et al.* (2019) [10]	IoT Security, IoT Protocols, Energy Consumption, Internet of Things, Synchronization, IoT Devices, Computational Power, IoT Network, Denial of Service Attacks, Energy Consumption, Synchronization Flood Attack, Internet Control Message Protocol flood, Energy Consuming Attacks, DoS Attacks, ICMP flood, CPU Usage, Energy Consuming Attacks, DOS Attacks.
Gurunath *et al.* (2018) [11]	Computer Crime, IoT Network Security, Internet of Things, IoT Expedients, Cost-effective Devices, Average Level Attacks, Low Graded Attacks, Safety Mechanisms, Cyber-attacks, Cybercrimes, IoT Protocols, IoT Bots, Power Consumption.
Soe *et al.* (2019) [12]	IoT Network Security, Internet of Things, Invasive Software, DDoS Attack Detection, IoT Environment, IoT Malware, Infected IoT Devices, Bot IoT, DDoS Detection System, Botnet Attack Dataset, Artificial Neural Network, Resource Constraint, Mirai, Public Dataset, Machine Learning, Synthetic Minority over-sampling, Imbalance Data Problem, DDoS Attack.
Xie *et al.* (2017) [13]	IoT Data Handling, Smart Power Grids, Smart grid, Power Engineering, Exposure Test, Power System Security, Blind Identification Approach, Attack Exposure Analysis, Low-sparsity Unobservable Attacks, Smart IoT, Data-driven Attack Scheme, Data Collection, Data Management, Relaxed Condition, Intercepted Meter Data, Attack Vector Construction, Sparsity-exploiting Method, Smart Grids, Transmission Line Matrix Methods, Covariance Metrics, Load Modeling, Transmission Line Measurements, Low-sparsity Unobservable Attacks, Attack Exposure Analysis, System Matrix, Data-driven.
Deogirikar *et al.* (2017) [14]	IoT Attacks, IoT Security, Internet of Things, IoT Vulnerabilities, IoT Security Countermeasures, Secure Communication, Encryption, IoT Architecture, IoT Attacks, Physical Attacks, Network Attacks, Software Attacks, Encryption Attacks.
Okul *et al.* (2017) [15]	Internet of Things, IoT Network Security, IoT Denial of Service Attacks, Man-in-t-e-middle Attacks, Invasive Software, Internet of Objects, Object Layer, Network Layer, Application Layer, Botnet, Computer Crime, IP Networks, Bluetooth, IoT Hacking, IoT Security Attacks, IoT Layers, Botnet, Data and Identity Theft, Denial of Service, Social Engineering.

CHAPTER 10

Improving Performance of Machine Learning-Based Intrusion Detection System Using Simple Statistical Techniques in Feature Selection

Abstract: An increase in cyber-physical systems and IoT has increased the output of the industry, and these systems have become the backbone of the industry. However, these systems are vulnerable to various cyber-attacks. The increasing number of IoT and cyber-physical systems has called for interventions in the way cybersecurity system works. This paper evaluates the effectiveness of various feature selection techniques– NB, LR, DT and SVM, ensembled shallow – RF and Adaboost with RBF and uses the statistical techniques Chi and Pearson correlation coefficient for choosing top features and applies them to the traditional machine learning algorithm to get accuracy and detection rate. The machine learning algorithms are trained and evaluated on the KDDCup '99' dataset. The study shows that machine learning algorithms work perfectly and provide higher accuracy if the feature vector consists of a few significant features.

Keywords: Deep networks, Ensemble learning, Hidden layers, IDS, Shallow learning.

INTRODUCTION

The world has seen the COVID-19 pandemic, and each walk of life has been affectedby it. Countries, governments, and native bodies emphasized preventing the virus from intruding into human bodies. If we glance at 2020, we will see that there has been an increase in cyber-attacks in India [1] and other geographies. Therefore, it is necessary to possess a reliable system that may sense the attack and take the required preventive actions. The preventive actions might startby alienating the machine, applying the antivirus, or informing the people that cyber-physical systems utilized in various operations are often saved. The attack's impact is magnified if there is an attack on the IoT systems of any industry. The typical methods show a limitation in stopping such attacks due to continuously changing impact methods and vulnerabilities. These attacks on IoT might be manual attacks, or the attack vector might be generated using some piece of code

Akashdeep Bhardwaj

or any technology. The increasing magnitude of attacks is often attributed to evolving hardware, software, algorithms, and dependence on cyber-related technologies for Industry 4.0. Better systems translate into more load on the system, more cyber traffic, and less time to categorize a malicious URL.

An intrusion detection system (IDS) was conceptualized to stop these attacks. The IDS [2] usually monitors the network and checks parameters like flow and network packets or reads the logs to detect any malicious or suspicious activity, bringing the entire system down. These IDS are commonly inflicted with a high false-positive rate and work poorly on unknown attacks. The unknown attacks are due to the changing network technology. It is imperative to make an IDS that may easily work upon new and unknown attacks efficiently. The ideal disadvantage of the normal IDS is that it is not self-learning and does not take necessary action unless it is specifically told about the principles and actions associated.

Machine learning (ML) algorithms have been found to be tackling such issues within the other problem areas, and thus, they are considered the golden key that resolves the problems of handling unknown attacks and provides correct classification with less error [7]. Currently, this paper is an effort to seek out the proper machine learning algorithm from commonly used algorithms and compare them. The input to the machine learning algorithm is typically a feature vector consisting of multiple features, and therefore, the classification algorithm is typically supported by the varied weights assigned to the features during a vector. The author is interested in using all the features of a vector and has tried to match the accuracy of the machine learning algorithms using only a few significant features selected through essential statistical techniques.

The normal IDS classifies the traffic into malicious or normal, supported by the given ruleset. These rule sets are not frequently updated; hence, normal IDSs cannot find the categorization, and they make an equivalent mistake till the rule sets are updated. However, machine learning-based IDS is sufficient for self-learning and categorizing unseen traffic with higher accuracy. The machine learning-based IDS is not hooked into the given ruleset, but it categorizes supported features and, therefore, the weight-related feature. Fig. (**1**) shows the schematic diagram for the IDS.

This paper is divided into 4 sections. Section 2 discusses the paper's foundation, various machine learning algorithms, the basic statistical techniques, and the performance parameters. Section 2 also discusses the previous work in the area and establishes the need to use statistical techniques to increase the accuracy of the machine learning algorithms. The dataset and experimental methodology are discussed in section 3. Results are discussed and analyzed in section 4, and the

paper ends by discussing the conclusion, shortcomings, and future directions or extensions of this research.

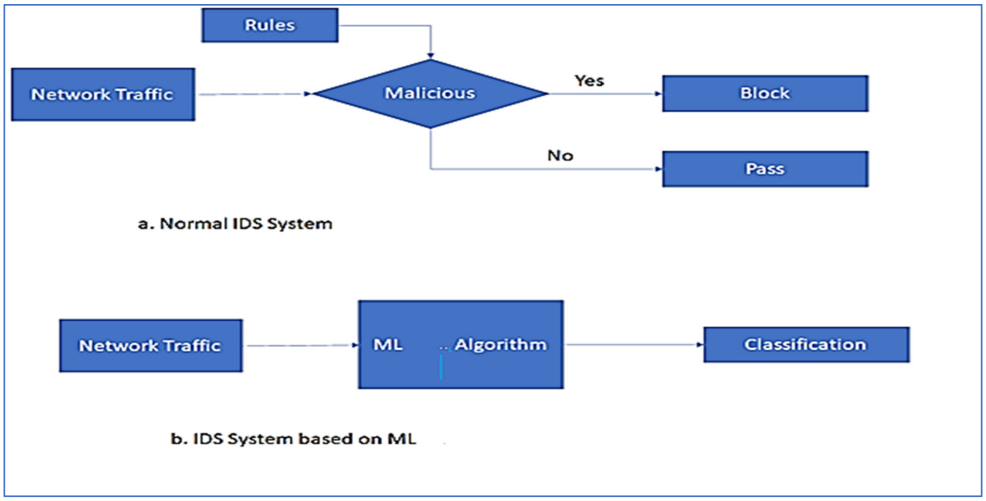

Fig. (1). Schematic diagram of IDS.

LITERATURE REVIEW

IDSs have been the center of research for the past few decades, and a variety of researchers have applied various techniques and tricks at different layers to stop tracts [4]. Few researchers have categorized the IDS into two types – signature-based and anomaly-based IDS (AIDS). Out of these two, signature-based IDS are prevalent within the industry.

Signature-based IDS (SIDS), the oldest generation IDS [5], has an inventory of the predefined attacks, and traffic signatures are matched to the signatures present within the list. They fail miserably if the attacks are not part of the list; list must be updated frequently. AIDS traditionally has an inventory, and traffic whose signature does not match the list is marked as attacks. However, machine learning algorithms can help AIDS identify unseen traffic as benign or malicious, and machine learning helps in AIDS self-learning.

Few of the researchers [6, 7, 8] bifurcate the IDS into network-based IDS (NIDS) and host-based IDS (HIDS). Both NIDS and HIDS have their advantages and drawbacks. For example, NIDSs are fast, but they tend to misclassify counting on the cryptography of the traffic, whereas the HIDS does not suffer from the cryptography of the network, but it requires all the configuration files to detect an attack. These research studies illustrated and presented that self-learning technology can be used as an accurate IDS.

SUBJECT INDEX

Akashdeep Bhardwaj

D

E

F

G

H

I

M

N

O

P

R

S

T

V

W

Akashdeep Bhardwaj

Prof. Akashdeep Bhardwaj is working as professor and head of the Cybersecurity (Center of Excellence) at the University of Petroleum & Energy Studies (UPES), Dehradun, India. An eminent IT Industry expert in areas, such as cybersecurity, digital forensics and IT operations, He mentors graduate, master's and doctoral students and leads several industry projects. He is a post-doctoral from Majmaah University, Saudi Arabia, and a doctoral in computer science from University of Petroleum and Energy Studies, Dehradun, India. He has published over 135 research works including SCI, Scopus, WoS papers, copyrights, patents, and has authored several books and chapters in international journals. Prof. Akashdeep worked as technology leader for several multinational organizations during his time in the IT industry. He is certified in multiple technologies including Compliance Audits, Cybersecurity, and industry certifications in Microsoft, Cisco, and VMware technologies.