International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Oct-2022)

https://dx.doi.org/10.12785/ijcds/120175

Issues and Solution Techniques for IoT Security Privacy - A Survey

Sripriyanka G[1] and Anand Mahendran[2]

[1]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India.*
[2]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India.*

Received 22 Jan. 2021, Revised 15 Jul. 2022, Accepted 23 Jul. 2022, Published 31 Oct. 2022

Abstract: The Internet of Things (IoT) is a rapidly developing technology that enables the interconnection of physical objects in our day-to-day lives. It integrates various smart technologies such as smart agriculture, smart cities, smart homes, smart healthcare, smart grid, smart industry, and so on. Physical objects are embedded with network and wireless technologies to exchange information without human intervention. It allows improving the experience of customers by detecting problems in applications. The current IoT technology brings unparalleled opportunities, accessibility, and productivity to smart technology users, but it also causes security and privacy threats. Frequently, these issues are related to data leakage and service loss in applications. Unfortunately, many of the commercial IoT products are not supported by strong safekeeping contrivances on confidential information leakage and unauthorized activities. It requires a modified high authentication and recovery architecture to secure confidential data from attacks. Numerous research efforts have been increased to reduce these security risks, but many challenges have not yet been solved in current smart applications. In this paper, we appraise security and privacy challenges and solutions for IoT smart applications in detail. This technological era needs to concentrate more on security with enhanced approaches and many existing technologies to succeed against threats. The security and privacy concerns of IoT-based smart connected healthcare applications are addressed, and we designed a bio-inspired optimization trained model to overcome the challenges. We have determined the recent explorations of the smart application's confidentiality and safety concerns through their controls theoretically. After the result of the analysis, we will focus more on the precarious issues with bio-inspired mechanisms, cryptography, and machine learning techniques for solutions with future directions in research.

Keywords: IoT, Security, Privacy, Bio-Inspired Mechanisms, Cryptography, Machine Learning

1. Introduction

A new revolution in internet communication is called the Internet of Things. The physical world that is linked to the internet is referred to as the Internet of Things (IoT). of Things" (IoT) was invented by the "Kevin Ashton" Auto-ID Center at MIT in 1999 [1]. Before IoT, computers had only brain memory without sense. In IoT, computers can sense the data and also send and receive the data from one machine to another machine without human interaction. There are a huge number of technological changes in our daily lives brought by this technology. The main goal of this smart technology is to support the things that should be interconnected all the time, anywhere, with everything by using the several pathways shown in Fig. 1 [2]. Billions of devices are connected to the internet for transferring information. Machine to Machine (M2M) connection taking to the next level called the internet of things. "Gartner predicts that the IoT will include 20.4 billion units installed in 2020." Sharing the sensor data between one object and another via the IoT gateway results in more efficiency and accuracy. This data collection can solve many types of real-world complications [3], [4].

In this digitalized period, a huge quantity of procedures is linked with the internet and the smart world. Here, smart has all sorts of applications. Also, develop and offer a huge number of objects and applications to industries and organizations. In the current era, IoT should occupy all sectors of human life. IoT applications can interconnect devices of universal accommodation with numerous networking communications to offer services efficiently anytime [5]. Groupings of various connectable devices can be interconnected and distribute the data from one to another. IoT technology is embedded with Radio Frequency Identification (RFID), actuators, sensors, Bluetooth, Zigbee, Z- wave, and Wi-Fi that interact and cooperate through protocol communication. Smart applications offer enhanced services to users with greater benefits. With this smart technology, customers achieve customized and seamless services from digitalized things[3]. An expansive variety of IoT usages are "smart farming, smart retail, smart home, smart building, smart city, smart healthcare, smart car, smart wearables, smart grid, smart parking, etc.". These intelligent

E-mail address: sripriyanka.g29@gmail.com, anandmahendran82@gmail.com

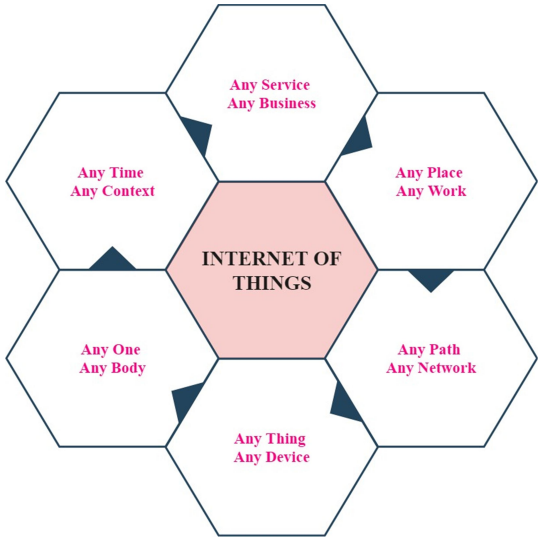

Figure 1. Strategies of Internet of Things

services can come with huge risks of security problems and loss of privacy. IoT developers failed to implement a strong security system on devices and applications with unsecured internet connections. For users, enormous safety and confidentiality concerns remain in the Internet of Things environment. Users place their personal information in private and public forums with good reason [6].

More numbers of network nodules, nodes of the device, and nodes of users are forming the multifarious communication link towards exchanging information. The ultimate aim is to identify and authenticate IoT applications by using cryptographic algorithms. The complexity of the IoT infrastructure needs more authentication policies while transmitting statistics from one thing to another [7]. Authentication for IoT security privacy is using hybrid mechanisms (such as cryptography techniques + lightweight protocols) and secret keys are updated every session securely [8], [9]. Lightweight encryption techniques and less complex encryption approaches are used to secure information in smart technology. In this technology, millions of sensors gather the statistics and send them to the server via the internet. But still, it requires an authenticated network to exchange confidential information between things [10]. The Attribute-Based Signature (ABS) technique necessitates accumulation and combining operations in the verification process and generating signature runs in the IoT network. In smart technology, servers (third parties) execute heavy calculations on other operations, but they leave a signature with fewer computations. Server aided computation technology (on signature verification) is used to increase the computation with low power and implement cryptographic operations deeply [11], [12].
Communicating with the internet directly for accessing data is one of the greatest encouraging devices in this smart era. Current routing protocols are susceptible to several threats and attacks. An Artificial Immune System (AIS) is used to discover the routing behavior of communication objects and classify the disobedient objects in the IoT infrastructure. The behavior of neighboring nodes is detected and secured intelligently by using enhanced AIS techniques [13]. It acts as a detector, identifying anomalies such as fake data and frank data. Bio-inspired-based cryptography algorithms provide robust solutions to computationally complex issues in data processing [14], [15], [16]. Many security risks are not addressed by centralized and traditional safekeeping approaches. A successful digital ant framework (a bio-inspired mechanism) was used to identify cyber-physical attacks in smart grid applications in the IoT [17], [18]. Analysis and monitoring of traditional approaches do not support the cyber-physical system's safety concerns effortlessly. The bio-inspired EvoSense system is simplified to detect attacks and failures early on in defense services. The ultimate aim is to execute the defense predetermined through defense service providers for abnormal behavior and malicious attacks [19], [20], [21], [22].
After a long time of practice, humans can be able to do the work correctly and get help from others if needed for a proper outcome. If we train our brains with the best knowledge, then we can start the work without help. Machine learning is an application of AI; it offers automatic learning ability to computers without any explicit programs. It is also known as statistics and a combination of computer science; it makes the machine get continuous learning and training for automation. This technology can use the available information (training data) to answer questions (prediction). The training of the machine can find the statistical pattern and learning features automatically for proper identification (output). Accuracy of identification depends on training information and the forcefulness of the machine learning model. If the data is more, the machine gets better learning and training for prediction [23], [24]. Likewise, more applications are being developed by using this technology. Currently, smart applications' security and privacy face huge and complex challenges from attackers. So machine learning (ML) classifiers and predictive analyzers are used to identify the attacks on current smart applications with proper learning [25], [26]. A single algorithm can't provide better security and privacy to users. We try to combine it with other technologies, and then we get better solutions to issues [27].
The main contributions of the paper are highlighted below:

- We scrutinize the security and privacy of the Internet of Things (IoT) to discover the main challenges and controls. We identify and reiterate the security privacy vulnerabilities and requirements for Internet of Things (IoT) technology.
- An information-rich survey on various aspects of IoT technology, including various IoT applications, four-layer IoT architecture with possible security and privacy attacks, and countermeasures.

- The feasibility of cryptography, bio-inspired computing, and machine learning is analyzed and reviewed for the security privacy of IoT applications. The potential use of these ubiquitous technologies is presented in the context of security and privacy enhancement in the IoT environment.

- A bio-inspired optimization model (BIO) is designed to detect malicious behavior in smart connected healthcare applications' communication and is beneficial in enhancing security, privacy, and network performance in digital healthcare infrastructure.

The remaining part of the review report is structured as monitors. Section II explicates the varieties of applications and devices on the "Internet of Things." Section III discusses the layered "structural design of the Internet of Things." Then, Sections IV and V present the layer-wise "safety and confidentiality disputes and solutions for the Internet of Things applications" in real-time. Section VI reviews some "enabling solution technologies for IoT security and privacy challenges, smart connected healthcare, and the bio-inspired optimization (BIO) model". And Section VII shows an "instantaneous" of our entire review. Finally, Section VIII describes some "future research directions and conclusions."

2. Internet of things applications

In this section, we discuss the wide variety of applications developed in IoT for customer usage. These IoT applications are highly reliable, save time and cost, and are well organized, as shown in Fig. 2 [3], [28].
Smart Homes are all connected with "Smart Thermostats." used to monitor the home and control the home's heating (and/or) AC conditioning. Thermostats are connected to the internet to allow adjusting the heating scenes by using network-connected devices like laptops, smart mobiles, etc. These systems can sense the surroundings and give alerts accordingly to the user's registered object. It has the capability to monitor the infrastructure automatically by using several cameras and sensors [29]. It offers easy and effective control of the home automation system via the internet, which decreases energy costs, and offers convenient services, and safety to the user. Smart appliances: these devices can be controlled remotely through computers, smartphones, etc. This will take some advantages of the smart world to make our work quicker, lower-priced, and more effective [30].

Industrial IoT (IIoT), the process of manufacturing consumes more energy, and greenhouse emission is highly contributed. But the smart industry enables the most useful interactions to achieve various enhanced goals and lower production costs [31]. The digitalized industry can transfer functioning data to manufacturers and engineers initially. The factory is managed remotely through the process of automation. It increases the efficiency of operations and worker protection [32]. Within the industrial environment, smart products are interrelated for self-processing, data storage, and communication. Various digital industries are offering their smart goods to customers by using automated industrial equipment and intelligent suppliers. Smart robots are developed to perform complex operations, and their use improves industrial productivity with secure control.

Smart wearable's, one of the major challenges in healthcare is providing equity healthcare services to patients in rural sections. Economically poor people may take a break for a regular health checkup. Smart devices with sensors can collect and analyze consumer data and send the information to other machinery about the consumer, and the goal is to make the consumer's life easy and more contented [33]. Emergency notifications are detected by using these smart devices and improving efficiency through wireless technology. Human daily activities are recorded for treatment, and real-time information is analyzed remotely on the public network for medical experts accessing it [34].

In Smart Healthcare, the main goal is to control and prevent human life with more efficiency. It can be used to watch the patients very closely and use the generated or sensed information for further analysis. A patient's psychological information is gathered via medical sensors [34]. Patient care quality is enhanced and efficient services are offered in smart healthcare with less cost [35]. This application allows people from various locations (e.g., patients, nurses, doctors, etc.) to get correct data and the best solutions for minimizing errors in the medical environment [36]. Remote healthcare monitoring is established with a Body Area Network (BAN) for health data collection, transmission, and processing. Alert applications provide enhanced services to patients in emergency times and can save human lives (especially elderly patients). This technology can use briefly tested classifiers for feature selection to protect the patients' health records and find the attackers in BAN [37], [38].

Smart Buildings control the operations in the entire building automatically by using sensors, actuators, chips, etc. We can use sensors to decrease the charge for energy and identify how many people are there inside the room, to adjust the Air Conditioning automatically, according to our room temperature. Smart technology mainly focuses to generate energy from renewable sources with less cost. It minimizes the heat in urban areas, and improves the quality of air and human life [39]. The overall building's operation control and monitor automatically according to ecological conditions [40]. Current technology developing a new dimension for the buildings to reduce energy wastage and increase safety mechanisms in emergencies [41], [42].

In Smart Farming, a joined sensor can help observe the temperature, light, humidity, soil moisture, etc. for the farmer. The most useful system in smart farming is an

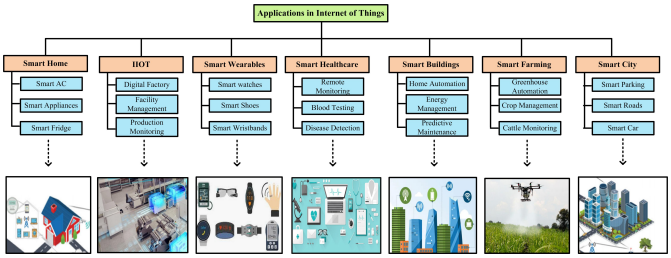

Figure 2. Applications of Internet of Things

automatic irrigation system. In agriculture, the traditional approach wastes water seriously because of evaporation and lacks soil information [43]. Smart agricultural databases, servers, and communication gateways play a significant role in offering on-demand agricultural services to authorized customers. The entire system is monitored accurately and according to various environmental conditions by using sensor information about the field [44]. Current farming infrastructure is developed to increase the crop yield and productivity of agriculture automatically. There is no need to visit the sites frequently for cropping and irrigation. It provides effective solutions to traditional farming by using advanced IoT technology [45].

Smart Cities will help us to improve sanitation, traffic reduction, environmental monitoring, and energy-saving [1]. Various urban services are to be highlighted in this application, such as performance, enhanced quality, and intercommunication for users. It improves the quality of life with integrated and automated communications technologies for citizens [46], [47]. Numerous devices for sensing and applications have been developed in smart city technology. Such as crowdsensing, street lights, smart grid, traffic sensing, smart car, etc. It shares common information about the network coverage area through wireless technology for providing effective services [48]. Information is collected by using sensors in real-time and analyzing that data for communication with decision-makers. Finally, it creates optimized solutions to improve the quality of the resident's lifestyle [49]. Smart cars use two different technologies (embedded and tethered) for automatic connection. These applications function remotely with programmed features for smooth, secure, and safe driving. The connected car is developed with energy-saving techniques, has a proper working schedule, is easy to park, and is well suited to city life. It becomes more efficient, intelligent, and powerful while improving its driving ability [50].

3. Internet of Things Layer Architecture

In this section, we discuss the structural design of the IoT divided into four parts: the sensitivity layer, web layer, interface layer, solicitation layer, and Internet of Things (IoT) security confidentiality mechanisms, which are shown in Fig. 3 [4], [2], [51].

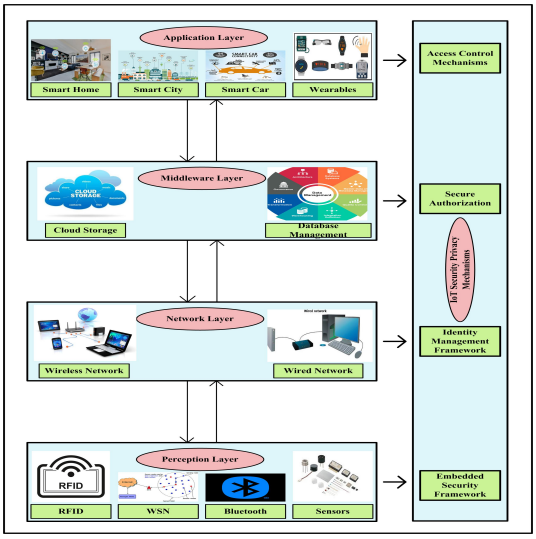

Figure 3. IoT Generic Layer Architecture

A. Perception Layer

This layer is executed at the bottom of the IoT structural design. That one is used to communicate with physical devices and machinery via smart applications such as RFID, sensors, etc. The foremost objective of the sensor layer is to connect objects on the Internet with their surroundings, collect this data, and transform the information from one smart device to another user interface. The sensitivity level is also known as the detector stratum of IoT infrastructure, and it follows some embedded security frameworks for protection.

B. Network Layer

This surface is similarly identified as the communication level for the IoT; it is implemented in the middle of the architecture. It is used to get the data from the perception layer and transform the data through combined webs. Many technologies are combined (wired and wireless networks) in this layer called "communication technologies" (such as Bluetooth, Wifi, RFID, NFC, etc.) and devices (such as gateways, hubs, cloud computing, etc.). The data is transmitted into many applications via gateways and etiquettes with an identity-based management framework.

C. Middleware Layer

This layer implements all the middleware machinery and applications of the IoT services. The middleware layer in the Internet of Things planning is used to interconnect the technologies "cloud technologies, centralized overlays, database management systems, or peer-to-peer systems". Various platforms and operating systems are run by the middleware layer, which also supports protocol standards for communications. It provides the most reliable communication to devices of heterogeneous and planned types with secured authorization.

D. Application Layer

This level is implemented on top of the IoT structure. Information is taken from the layer of the network and uses the information for operations (services). These layers offer storage services to do the backup process and databases for future use. For example, smart cities, smart homes, smart farming, smart healthcare, smart grid, smart transport, etc. These applications are accessed with some secured control mechanisms to protect them from unauthorized activities.

Four-layer architecture designs show the plainness of multiple-layer planning of the IoT. The network layer not only finalizes routes and transforms the information, but also provides the services called aggregation of data, computing, etc. The application layer provides the service (information mining, information analytics, etc.). [6], [52], [28].

4. Internet of things security issues and solutions

In this section, we discuss security as the defense of information from threat activities. It includes the prevention and detection of information by using tools, services, and policies. The application is secured from vulnerable activities such as access, steel, and information modification [53], [54]. Current era devices are connected to the internet for interchanging data, called the "internet of things". It carries new types of risks like secrecy and privacy. The industry and supply chain of the web of things must consider the challenges. Web-connected devices always come with a high demand for security features for IoT strategies [7]. Here we need to demonstrate vulnerabilities in end-to-end Internet of Things secrecy calculations [55], [56]. Also, minimize the risks and provide the best solution by using approaches called cryptography and bio-inspired mechanisms. Platform modules are secured by using a chip, which is used to protect the sensitive data of users; licensed anti-virus software can run on our internet system. Devices with this technology always attract hackers. Internet of Things exchanges the data on a public network; unauthorized users that are attackers can access the confidential information. So we need to encrypt the information by using the cryptography approach and forward it to the receiver. In this section, we discuss IoT security and controls shown in Fig. 4 [4], [57], [28].

A. Application Layer Security

The application has poor coding and design, which means it is caused by security problems. For that, we need to develop the application with a better design and also consider the issues of IoT applications before launching them. It also gave clear information about the application as well as security problems for users' better understanding. And better practices and awareness should save our applications from threats. So our goal is to secure our applications from hacking. Here we discuss the security attacks and controls on the internet of things applications.

1) Application Layer Security Attacks:

a) Denial of Service:

Current day IoT is used by most people, but services are denied by offenders. In the Internet of Things, this attack aims to interrupt the connection between readers and RFID tags. In 2017, security researcher Ruben Santamarta clearly showed the problem with Norwegian Airlines' WiFi service [58].

b) Malicious Code Injection:

It is the procedure of inserting the hateful program addicted to the net link, and then the entire system is controlled by hackers. The central determination of the eruption is towards bargaining with this customer data, spreading worms. Then the entire system will shut down after this attack. It had many types of injection attacks (shell injection and HTML script injection) to hack the many types of IoT applications [28].

c) Spear Phishing:

This attack targets a particular IoT organization's electronic mail and communication for malicious program installation. Even though we get an email from a trustworthy source, it takes us to a bogus website full of malicious programs. Sometimes government-sponsored hackers also do these spear-phishing attacks by using highly designed social engineering techniques [57], [59].

d) Sniffing:

The attacks aim to capture the network packets and make an interception between a reader and an RFID tag while transferring the information on the IoT applications. Here, a criminal needs to hear the authorized person's telephone calls to get the secret data by using bugged telephone lines [57].

2) Application Layer Security Controls:

a) Access Control:

Access control on IoT applications improves the security level against hackers. It supports tractability and scalability on the internet of things. This provides access control key tokens to the users for security purposes, those who use the internet of things.

b) Authentication:

The security point of view needs to certificate our IoT devices (both sender and receiver) [60] by using some lightweight authentication approaches, such as public key infrastructure (PKI) strong two-way authentication. Use it to ensure the authentication of the user's applications on a public network [2].

c) Cryptography:

It is a popular technique (Elliptic Curve Cryptography) to secure the internet of things transactions. This mechanism, used to protect IoT systems from side-channel attacks, also offers the best solution for security problems and reduces the burden of computation [61].

d) Key Management:

Key management steps happened only in a secure manner. It contains the creation of the key, the spreading

of a key, the packing of the key, and the informing and mutilation of the key. If the key and the certificate have expired, the application may shut down. The complexity of the cryptography approach is in proper key management and certificate maintenance with regular updating. So, key management is more important for IoT devices. It is almost required for secure communication on IoT sensor nodes and encourages security authorization [57].

B. Middleware Layer Security

Powerful computing services and more storage space are provided by this layer in the IoT environment. Also, this layer was hacked by numerous assaults. These outbreaks can regulate the whole solicitation, via the spread of that malicious code. Many possible attacks were discussed in this section [62].

1) Middleware Layer Security Attacks:

a) DoS & DDoS:

A distributed denial of service attack (DDoS) is the same as a DoS attack, but it targets many IoT systems for distribution purposes [28]. The goal of this attack is to break the accessible resources and also make the network of resources unavailable [57].

b) Malicious insider:

In this attack, unauthorized persons (attackers) are on the network or IoT devices with authorized access control. In 2016, cybersecurity identified 60% of attacks caused by insiders; of these, 44.5% were attacked by malicious insiders. For example, in healthcare, authorized employees (admins) had all authority to modify the patient's treatment details. Here, this person may reveal the patient's treatment details to unauthorized users [63].

c) Malware injection:

In this attack, malicious programs are injected into virtual machines (VMs) and sent to the IoT cloud system to spread the malicious data throughout the entire application, which also affects the overall functionality [57]. Finally, an attacker can get confidential information about the system service [28].

d) Unauthorized access:

Since the IoT had fewer storage capacities, it used the cloud to store a large amount of information with proper access control. These attacks affect the exact functioning and unauthorized entrance controllers on the IoT devices [61]. In the RFID tag's absence of appropriate authentication, information is deleted or modified by attackers easily without authorizing right of entry [64].

2) Middleware Layer Security Controls:

a) Access Control:

Already, explained in the previous section.

b) Anti-malware:

The particular software is designed to identify, safeguard, and delete the malware on IoT applications. This will scan the files continuously also looking for a known type of threat. If malware is detected means immediately alerting the applications and protecting them from threats [57].

c) Intrusion Detection and Prevention System (IDPS):

Most efficient prevention and detection approach for the activity of malicious. This system is used to monitor the activities of users, web, and processor systems for intrusion detection and preclusion. Generally, IDPS can replace or remove the vulnerable part of the IoT application [65].

d) Moving Target Defense(MTD):

This MTD method increases the attacker's cost and complexity by enabling continuous change of applications (environments). Optimization problems are solved by using automatic configuration and the efficiency of application secrecy is improved in this approach [66].

C. Network Layer Security

This layer is used exclusively to transmit data from one object to another. Here, data interchanging is dependent on the web without humanoid interaction. In this case, implementation of security is more difficult. So we need to develop and use highly secure communication protocols for communication. Then IoT applications must be protected from intruders. This section explains network layer security attacks and controls in detail [67].

1) Network Layer Security Attacks:

a) DDoS & Malicious Code Injection:

DDoS and Malicious Code Injection were discussed previously.

b) Malware:

It is malicious code or software created by aggressors to damage and spread viruses in the IoT environment. It includes spyware, Trojan horse, botnet, etc. [57].

c) Man-in-Middle(MIM):

Unauthorized users (hackers) can yield the controller of the complete IoT solicitation without authorized user knowledge [62]. A very dangerous attack on network announcements and MIM work as a malicious postmaster. He/she changes the actual content (sender data) sent to the receiver and also closely connects with both users for data access control [68].

2) Network Layer Security Controls:

a) Anti-Malware:

Security point of view the IoT system has less functionality. We go with this approach because it is also a piece of software. After installing anti-malware on our device, it detects and protects the system through continuous scanning. This protection can be used to prevent crucial data from being assaulted while in communication.

b) Firewall:

Use to protect the technology from illegal users. This functionality can protect smart objects and provide a better solution [69]. One of the casual techniques to manage network protection [70].

c) Intrusion Detection System(IDS):

This method continuously scans the IoT application to prevent malicious activity. It is used to find errors, bugs, and intrusions on a device [71]. IDS works in three phases. The

first step is monitoring the application. Second, step analysis and finally detect the intrusion in internet applications [72]. This system alerts the user after the identification of malware by making an alarm on secure internet devices [73].

d) Key Management:

Key Management is illuminated in the previous section.

D. Perception Layer Security

One of the most important impressions in the IoT approach is the perception layer security used to collect information from another layer. This layer senses the useful information on smart objects by using sensors, RFID tags, and Actuators for data transformation in a secure conduit [74].

1) Perception Layer Security Attacks:

a) DoS:

Denial of Service security attack is explained before section.

b) Message Replay:

An unauthorized person stores confidential information from the RFID tag without authorization. Later retransmit the stored data and make unauthorized activities (duplicate transactions, etc.). This type of attack can threaten fresh message transmission [75].

c) RFID Stealing:

RFID technology is used broadly in many fields. It has three phases: surveillance, tracing, and controlling. Without authorization, aggressors can bargain with the data from RFID tags. Unprotected tags are hacked easily by hackers. Because high-cost IoT applications don't have appropriate refuge maintenance [76].

d) Sniffing:

In general, it is used to analyze and test the usage of networks on IoT devices. The attacker can interrupt the communication between authorized users and do vulnerable activities. Zigbee network technology doesn't use any encrypted approach also vulnerable to this kind of attack [77].

e) Spoofing:

In unauthorized access control of IoT devices spoofing attacks are launched easily. These kinds of overhearing attacks happen, while the information comes from an authorized RFID tag [77].

f) Tag Cloning:

Here hackers can improve access control on sensitive information from IoT applications and the same time very hazardous for the company's status [78]. Also, the cloned device is implanted into the original RFID tag for threatening [57].

2) Perception Layer Security Controls:

a) Hash Lock:

This technique can present two conditions for security attack control. Those who answer all queries with a correct hash value are called a locked state. Another one is to perform the usual operation called unlocked state [78]. In cryptography, a much hash-based encryption algorithm is designed for IoT security control.

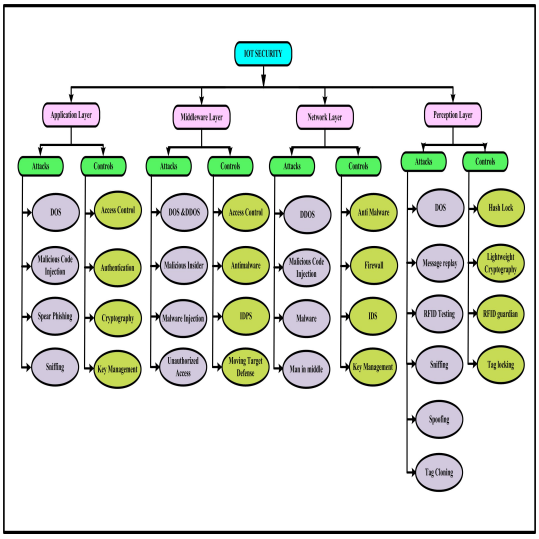

Figure 4. IoT Security Issues and Solutions

b) Lightweight Cryptography:

Many lightweight cryptographic concepts are used for security concepts on IoT. Fundamentally, the RFID tag has less storage capacity so we go with this approach. This offers secure manner communication between smart objects with less energy consumption [79], [80].

c) RFID Guardian:

To protect the RFID tags from unapproved readers. This is also a better solution for complex issues in IoT applications. The secure RFID mechanism is more dependable also much faster in data transferring. It is a battery-powered device [81], [82].

d) Tag Locking:

An RFID tag is locked (protected) by using the PIN to protect the data on communication. Once locked then can't able to transfer the information. When the access PIN is matched with the original tag's number then only unlocked for transformation [81], [82].

5. Internet of Things Privacy Issues and Solutions

In this section, we discuss privacy as the control of personal details by using authentication credentials. It is used to establish the boundaries of our confidential information for access control. Security and privacy have become major problems in smart technology [53], [54]. The development of consumer IoT products needs to raise awareness about privacy risks to the clients. This technological growth has privacy issues. Hackers can access confidential information without any permission from the consenting user. We need to protect the data and also consider issues of privacy in the IoT environment [61], [56]. In this section, we explain the IoT privacy attacks and controls shown in Fig. 5 [52], [57], [28].

A. Application Layer Privacy

These segments explain the confidentiality dangers of this IoT solicitation stratum. These kinds of applications are hacked easily by more precarious attacks.

1) Application Layer Privacy Attacks:

a) Confidentiality Threat:

This type of threat can expose confidential data in an unauthorized manner. In IoT, routing details can be threatened by attackers and damage the device [83]. Hackers need some secret details like PIN, secret keys, etc. so simply enter inside and analyze the applications.

b) Identification:

Identification point of view internet technology can use many technologies, smart cameras, fingerprints, etc. These applications are threatened by the adversary; also get the access details for personal data collection.

c) Profiling:

This system is used to store personal details in the public forum with privacy. But public service providers sold secret data on marketplaces (for advertisement) without our knowledge; hackers can identify the group or person easily for profile hacking [57].

d) Tracking:

In the technological era, we share our details by using smart things. These will store our data on social networks without proper privacy. So, eavesdropper easily tracks our secret data with undesirable revelation for location identification.

2) Application Layer Privacy Controls:

a) Anonymization:

It is one type of privacy protection system for smart application users. Here anonymized information can't be re-identified, if tried by an attacker also anonymous party (organization) gets alerted through a message. They are the authorized persons for our confidential data.

b) Data Masking:

It is used to transfer and maintain a high level of crucial data on IoT applications. Always, exchanging the copy of actual information with some mask also protects the user's data [57].

c) Privacy-Preserving Authentication:

An authentication point of view, create fake identification for original users by using cryptographic communication protocols deprived of illuminating actual details. Here we use lightweight protocols for encrypted privacy-preserving; IoT applications had the lowest storage capacity [84].

d) Pseudonymity:

This method slightly differs from the anonymous method for identification (it requires re-identification) in IoT systems. The pseudonymity technique uses a puzzle-solving approach for high authentication while transactions are in real-time. So we need to access the data means to solve the cryptographic puzzles correctly [85].

B. Middleware Layer Privacy

These layers provide efficient interaction between the IoT applications with protected privacy for users. In this section, we discuss the attacks and controls on the middleware layer in IoT.

1) Middleware Layer Privacy Attacks:

a) Excessive Data Storage and Processing:

In IoT, we need to store and process more sensitive data while in communication. The attacker can access our data in an uncontrolled manner while exceeding application storage. Also, it increases the possibility of hacking and data theft.

b) Inference:

In IoT, attackers can identify the users' background information through data exploitation. To launch the inference attacks, an adversary can identify the untrusted information in offline transformation [86].

c) Information Leakage:

On a public forum, our personal is under the control of service providers. Attackers easily can access the leaked personal information (unprotected files) on IoT devices collected by sensors. Continuously hackers can monitor the unruffled details on smart applications for misuse [87].

d) Unauthorized Direct Data Access(UDDA) :

Authorized IoT users can store the details on cloud storage. But this sensitive information is hacked or vulnerable by unauthorized users.

2) Middleware Layer Privacy Controls:

a) Active Data Bundles(ADB):

This control method is a software-based approach and interfaces metadata, sensitive data, and virtual machine. ADB privacy control mechanism is used to prevent and protect user information on IoT applications. Also, it offers effective and efficient data privacy protection to smart healthcare applications. It supports secrecy information migration on distributed infrastructure [88].

b) AB Access Control:

Offer attribute-based (AB) encrypted access control to authorized IoT users on communication. It contains attributes, devices, and users to protect confidential data from unauthorized users on smart things.

c) Homomorphic Encryption:

This type of encryption approach is very powerful in preventing unauthorized accessing of data. The attacker can't able to identify the actual data on this encryption approach. It will use simple calculations for encryption and authentication on IoT applications [89].

d) Personal Digital Rights Management (PDRM):

It is self-oriented prevention and protection approach for penetrating information. We need to install the detector (software) for personal data protection. Also, it is used to recognize the unusual access and denial of accessing data.

C. Network Layer Privacy

This division describes an utmost treacherous network layer confidentiality attacks and most encouraging control mechanisms [90].

1) Network Layer Privacy Attacks:

a) Camouflage:

Attackers can hide the vulnerable node by using the camouflage method on the IoT network environment also compromise the communication between nodes. It transfers the wrong data to the users and gets the original data for privacy hacking [77].

b) Confidentiality threat:

The confidential threat concept is discussed before the session.

c) Eavesdropping:

IoT devices are communicating with sensors for information delivery. So, an eavesdropper can interfere and send the malicious code with sensory data. This kind of attack can monitor the entire system for snooping. The foremost objective of these outbreaks is to get these sensory details from those authorized connections while the user transferring [77].

d) Traffic Analysis:

In IoT, network attackers can interrupt the flow of data to abstract secret information. Unintentionally RFID tags are responding to hackers in this privacy attack [91].

e) Juice Jacking:

A type of cyber attack, involving data/charging cable for malware installation and thieving confidential information on IoT applications. These attacks present a big threat to users' privacy with a lack of awareness. It may lock the device and export information/ passwords directly to the scammer[92].

2) Network Layer Privacy Controls:

a) Digibox:

It is a container-based protecting approach for the IoT host connection between the network nodes. We need to use some cryptographic algorithms to generate digital-based encryption for applications' privacy protection.

b) Dummy Traffic:

It controls the traffic analysis attack on smart applications by using dummy data packets. This will make available dummy nodes to fleece the original information.

c) P2P Encryption:

Encrypted information send to another user, the receiver can decrypt the unreadable information autonomously in Point to Point (P2P) method.

d) Priv-code:

IoT users' information should be protected by using session keys. If the user can type the session key (One Time Password) correctly then use the secret details. We use cryptography algorithms for conference key generation.

D. Perception Layer Privacy

We explain the details about the perception layer privacy attacks and controls [90].

1) Perception Layer Privacy Attacks:

a) Eavesdropping:

This concept is reviewed in the last session.

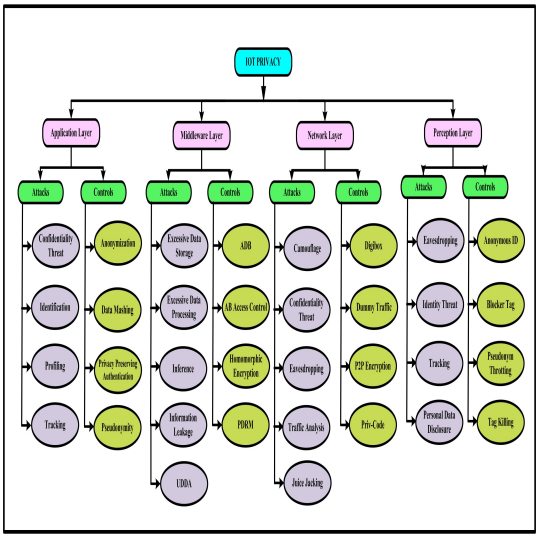

Figure 5. IoT Privacy Issues and Solutions

b) Identity Theft:

Hacker (theft) can take someone's personal information to track or monitor the person dishonestly.

c) Tracking:

Tracking is explained in attacks on application layer privacy.

2) Perception Layer Privacy Controls:

a) Anonymous ID:

This privacy control system is discussed already in the security control section.

b) Blocker Tag:

It is used to block the tag when the tag responds to the attacker without the knowledge of the owner. This will offer the best privacy protection to the user from unconstitutional activity.

c) Tag Killing:

If the device identifies malicious activity on the RFID tag then kill the tag. So, the attacker cannot able to hack our device.

6. Enabling technologies for IoT challenges

This technological world is introducing numerous challenges to security and privacy in smart applications. Enabling technologies are used to secure and save IoT applications in the public network [93], [94]. Such technologies are cryptography, bio-inspired mechanisms, and machine learning, all discussed in this section.

A. Cryptography Techniques For IoT

The latest technology mostly uses RFID tags for collecting data and transmitting it to remote smart objects. Since these tags had very few computational capabilities, they also suffered from heavy computations in IoT systems, as explained in table 1. In this case, attackers easily access information and compromise privacy, also creating forgery problems on devices [95]. To get around these difficulties,

we use lightweight encryption algorithms when compared to traditional algorithms. For several reasons, we secure communication and information transmission in the IoT infrastructure. In this fragment, we appraisal lightweight cryptographic procedures intended for this internet of things stimulating issues.

B. Bio-Inspired Optimization For IoT

IoT applications require strong optimization techniques for security and privacy challenges. A security and privacy solution in the traditional approach is infeasible to provide exact results to the threats in IoT technology. It had very limited computing resources. Devices can be damaged unpredictably and memory is restricted in communication technology [101]. This review in table 2 has proposed an enhanced bio-inspired optimization framework for IoT security and privacy theoretically. Bio-inspired optimization techniques are more efficient and effective than traditional approaches. Smart technology always finds optimal solutions to resolve complex problems in smart technology. It is used to solve the security issues in IoT applications and also provides decentralized safety [20], [21].

C. Machine Learning Techniques For IoT

The "Internet of Things (IoT)" is integrating sensible items through network communication for providing intelligent and enhanced services to the users [104]. Smart technology is facing more challenges in security and privacy shown in table 3. In this IoT technology, we need to secure the connected devices and information collected via wireless sensors. Existing traditional approaches are not enough to prevent and protect IoT devices from threats. Machine Learning (ML) based solutions are used to detect smart attacks [105]. It provides intellectual services to IoT security and privacy challenges with secured communications. A past attack on IoT security and privacy is used to improve the solutions via continuous learning in this technology [106]. ML is one of the emerging technologies to address privacy and secrecy issues in smart applications with appropriate solutions [107]. It predicts the network threats on IoT applications by previous learning methods. Machine Learning-based enhanced new architecture is facilitating IoT devices to detect and prevent attacks[108], [109].

6.1 Security and Privacy Issues on Smart Connected Healthcare

In healthcare, diligence, and smart skills have frequent applications. This smart technology is used to offer superior quality medicinal services to the users and collect health-related information (e.g., blood pressure, sugar levels, and so on). Through wireless sensor communication, the patient's real-time data is collected and sent to the physician. Also, smart connected healthcare expertise can provide comfort in supporting and observing the vigorous information that can aid in decision-making in the clinical sector. And the doctor of medicine can examine the patients' illnesses and generate a prescription digitally,

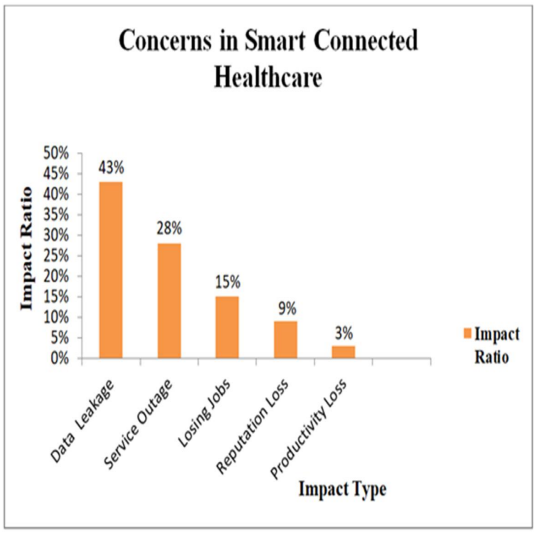

Figure 6. Concerns in Smart Connected Healthcare Application

which is sent to the users. This skill can assist in real-time by watching the patients tenuously, providing effective healthcare facilities to the patients, reporting the patients' emergencies appropriately, and potentially saving many individual lives [110], [111].

Particularly personal data processing and discretion are concerned in connected healthcare infrastructure. Need to ensure the protection of patients' privacy and security is provided by the digital healthcare suppliers. And safeguarding the patient's private information that is collected by the wireless technology and used legitimately but reasonably from prospective misappropriation.

Patient privacy is a major challenge in smart connected healthcare. In smart healthcare solicitations, an enormous amount of information is collected continuously from patients. These patient details are breached, malformed, and imitated by unapproved parties using malware such as jamming, spoofing, cloning, and so on. In smart healthcare, radio frequency jamming is a malicious activity that interrupts the functionalities of patient activity monitoring systems, and sometimes it may cause the loss of patient life [112], [55].

In man in the middle attack, unauthorized commands are mixture directly keen on smart healthcare devices for redirecting the services. To risk the patient's lives, hackers can launch DDoS attacks on intersecting digital health services. The inaccessibility of security and privacy standards for digital healthcare devices is one of the major concerns in the connected healthcare environment. Various safety and isolation attacks are not apprehended or identified by the users. In smart connected healthcare, secrecy and confidentiality are the foremost anxieties for both physicians as well as patients [113], [114]. The major and most impactful threat in connected healthcare is data leakage. This results

TABLE I. CRYPTOGRAPHY TECHNIQUES FOR IOT CONCERNS

S. No	Citation	Author & Year	Cryptographic Techniques and Protocols	Limitations	Advantages	Future Work
1	[96]	Sherali Zeadally et al. & 2019	RSA with PKCs AES with CMAC Various encryption protocols	1. To authenticate every message in IoT applications. 2. Suitable only for smaller key lengths.	1. Provide secured access services to the IoT users. 2. Secure transmission of smart objects.	Lightweight public key-based ECC cryptosys-tems.
2	[97]	Inayat Ali et al. & 2016	ULA(Unique Local Identifier) Kerberos authentication ECC	1. Generally, traditional cryptography algorithms have more CPU power and consume high battery energy.	1. Lightweight pro-tocols provide high-security services.	To develop new security solutions for IoT applications.
3	[98]	Yang Lu et al. & 2019	Role-based access control (RBAC) Secure data aggregation in WSNs, such as SEDAN Kaos, Tropos, NFR, GBRAM, and PRIS	1. Novel safe keeping concerns and new technology users' isolation problems are carried through IoT infrastructure but the traditional safety measures are not effective for those anxieties. 2. Safekeeping concerns openly disturb the advanced development and application of IoT.	1. Cyber security guarantees these [IoT] will develop a protected linkage for the societies. 2. These mechanisms provide high security and privacy to IoT applications.	The future direction of cyber security issues and Potential solutions.
4	[99]	Rajat Chaud-hary et al.& 2019	LB-PKC techniques	1. The customary-based cryptographic procedures and set of rules are not effec-tive to switch the re-treat and confiden-tiality experiments in the IoTs atmosphere since they did not strongly towards the significance of as-saults.	1. LB-PKC techniques are protected from quantum attacks.	Biometric-based endorsement conventions and lbc procedures are used in smart IoT solicitations.
5	[100]	Manisha Ma-lik et al. & 2019	Key delivery Crypto-graphic methods Au-thentication schemes	1. Still, security for IoT is in its infancy. Lack of advanced se-curity services Com-plexity of key man-agement.	1. The secure key bootstrapping approach offers better communication on IoT.	Plan to optimize asymmetric key protocols and post-quantum cryptography key exchange.

6	[9]	Kim-Kwang Raymond Choo et al. & 2018	FHE Lightweight certificate less autograph pattern to confirm records truthfulness in IIoT structures	1. Technological changes will produce extraordinary chances alongside novel hazards to the public.	1. In healthcare improve access to patient's data for an immediate treatment plan. 2. Also, diminish vitality ingestion and develop accurateness.	Frothy cryptographical encryption structures for the concrete assaults in contrast to Industrial IoTs schemes.
7	[12]	Satyabrata Roy et al. & 2019	Algorithms are developed with group-based cellular automata [GCA] called "LCC (lightweight ca cipher)". Also, its position for smart technological solicitations and strategies information safety and isolation.	1. "Symmetric-key encryption" techniques are suffering from key controlling complications.	1. LCC technique prevents data theft from communication on perception and network layer.	1. LCC technique prevents data theft from communication on perception and network layer.

in patient information being compromised. These threats in connected healthcare devices are represented in fig. 6 [38]. For optimal solutions in smart connected healthcare infrastructure, security principles and methodological qualifications still need to be improved. To ensure extreme protection of patient data privacy, authorized access control should be implemented on digital healthcare devices [55]. During patient record transmission and loading, encryption methods provide data defense from hacking activities. In the healthcare region, security regulations and policies play an essential role in protecting transmission between patients and medical practitioners [115], [116]. Patient information can contain sensitive details such as the type of disease, mental status of the patient, identical information, and so on. This information needs to be protected from hacking and malicious activity, even if the patient's information is interrupted and apprehended. Consolidated supervision is used for attack and network monitoring in digital healthcare applications. Artificial Intelligence (AI) based technique is established and arrayed for averting the safekeeping extortions in real-time [38], [114].

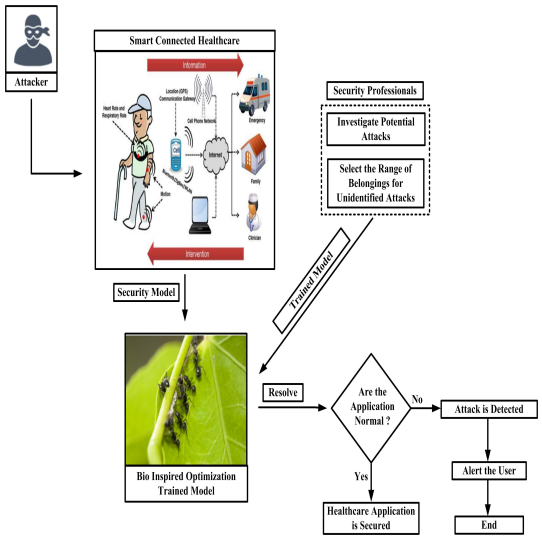

Figure 7. BIO model for Smart Connected Healthcare Application

6.2 BIO Model For Smart Connected Healthcare Applications Security

The smart connected healthcare application pays to improving the daily life facilities and handling the great quantity of records stream but raises the safety and confidentiality concerns while the data is in communication. For handling these security challenges, an essential computing paradigm needs to be developed to handle these security challenges. Several security and privacy procedures, namely the implementation of cryptographic algorithms and machine learning, demand a significant amount of parallel processing. Most of these medical IoT nodes lacked inherent cryptographic and other primitives due to restricted computing capability (e.g., restricted CPU ability and storage), so computation can indeed be concluded within these sources of energy contexts. Because there are no strong encryption systems on all devices, they are vulnerable to replicated assaults.

In smart connected healthcare applications, attackers try to attack the connected devices for stolen information about patients or humans who are having health issues by using sensors. In Fig 7, we provide the Bio-Inspired

TABLE II. BIO-INSPIRED OPTIMIZATION TECHNIQUES FOR IOT CONCERNS

S. No	Citation	Author & Year	Bio-Inspired optimization approaches	Limitations	Advantages	Future Work
1	[20]	Mohd Faizal Ab Razak et al. & 2018	Particle Swarm Optimization (PSO) Evolutionary Computation	1. The attacker identifies the user data for hacking. 2. Malicious code can hang out the entire application.	1. Increase the performance of Android Malware Detection.	To detect android malware on the cloud.
2	[21]	Alan Oliveira de Sa et al. & 2017	Backtracking search optimization algorithm PSO	1. Infected data should be transferred via signal. 2. Attacker use malware injection on signals	1. Improve attack identification 2. Continuous Scanning for attack detection	To investigate countermeasures to recognize and preclude Lively Structure ID assaults.
3	[102]	Usman Rauf & 2018	Swarm Intelligence Human Immune System Genetic Mutation Biological Regulation	1. Due to the non-adaptive behavior of present structural design, they stay neither vigorous nor spirited on attacks. 2. Only they have restricted wisdom competence and do not acquire new unexpected situations also continuously changing the environment. 3. The current device doesn't realize the risks.	1. These approaches manage large networks efficiently from attacks. 2. Identify the threats automatically after training.	To implement the genetic mutation algorithm for DDOS attacks on devices.
4	[103]	K. Munivara Prasad et al. & 2017	Cuckoo Search Algorithm	1. Distributed Denial of Services attacks is profoundly carried out and focused by the attackers on the layer of applications threatening.	1. The bio-inspired approach is to prevent the application from HTTP flood attacks.	Other than single bio-inspired procedures are used in the forthcoming hybrid approach to delineate the new abnormality based on contrary flood violence exposure.
5	[15]	Charles O. Muango et al. & 2019	Firefly Algorithm	1. Node injection attack is the most difficult to detect whereas internet worms are invented every day due to detection limits. 2. The intervention of third party solutions cannot be applied uniformly as this will increase the whole rate of the structure.	1. These authors can classify these attacks in terms of efficiency and damage	The characteristics of the light intensity that can be best suited to repel intruders at the same time allow for the incorporation of devices in the same domain. Investigate more security. Also, we shall work to build this architecture and test it in a real environment.

6	[16]	Sahar Aldhaheri et al. & 2020	Artificial Immune Algorithms	1. The destructive collection approaches are used for circulated and inconsequential techniques but this cannot be accessible or appropriate towards the composite conditions.	1. AIS too successfully applied towards solving multi-objective optimization problems control engineering and robotics.	Rectify the adaptability issue also the Huge Dishonest Progressive Rates. An additional fact is to build up a propelled methodology, for example, uniting other than unique AIS calculation or with further bio-roused techniques.
7	[13]	Kashif Saleem et al. & 2017	Nature learning-based protection structures with routing-based protocols for IoT infrastructure.	1. Currently, IPV6 protocols for IoT are easily prone to numerous exposures.	1. It offers edge to edge security to IoT application users. 2. The behavior of neighbor nodes should be detected intelligently.	Novel BSCoP changes the metrics through variations of protocols for analysis.The output of the real deployed testbed is performed widespread simulations proceeding this solicitation.

Optimization (BIO) based trained security model which overcomes the above issues by investigating the attacks with privacy concerns. In this paper, we explore the new model to detect known and unknown attacks using a bio-inspired optimization (BIO) technique.

6.3 Summary

In this survey, we compare literature on the issues of security and privacy in the smart connected healthcare application; it investigates the taxonomy to fulfill the criteria for control and authenticating the patient's data based on the following scenario.

- Bio-Inspired Optimization (BIO) is used to evaluate the application among the assessments and contrasts.

In the first phase of the work, we used the security and privacy constraints to examine the security and privacy constraints using security professional attack detection mechanisms to determine whether the smart connected healthcare application is working normally. The primary goal of the scenario is to train the model for the security and privacy limits of patients with probable data records. The foundation for the adaption of security and privacy would be the same for patients with chronic conditions, but in pandemic situations, collecting information about suspicious records is critical.
The Bio-Inspired Optimization (BIO) specifies how another sort of data will be treated based on its optimizing parameters, such as anonymization, the significance of data protection, controller, consent, and operator. The BIO-trained model investigates the potential attacks and manages the normal flow. To examine the smart connected healthcare application model, the following parameters are essential to training the BIO model, and these parameters are more useful to optimizing entire smart connected healthcare systems, which we describe below.
Topology (hospital network), interoperability (using the smart environment where people transmit the data between the information systems and IoT devices), policies (accessible control within that context as well as specifying what data will be transmitted among devices and systems), risk (the risk is an anticipated number that takes into account the likelihood of harm occurring as well as the degree of the damage), and hierarchy (several surroundings as well as numerous encounters between both the patient and other providers and devices).

7. Outline of the paper

In this review, the authors have investigated the privacy and security issues and solutions in IoT applications and devices. The purpose of this survey is to find out the optimized solution need to be addressed on smart technology challenges. Successfully addressing security and privacy issues in smart applications is a more challenging task. We reviewed various emerging solution techniques (cryptography, machine learning, and bio-inspired mechanisms) for real-time IoT security and privacy challenges. We design bio-inspired optimization (BIO) trained model to improve the accuracy of attack detection in smart connected healthcare applications.

8. Conclusions

IoT technology changes a lot in human life every day with numerous smart applications and devices. Various

TABLE III. MACHINE LEARNING TECHNIQUES FOR IOT CONCERNS

S. No	Citation	Author & Year	Machine learning Techniques	Limitations	Advantages	Future Work
1	[104]	Liang Xiao et al. & 2018	All types of machine learning techniques are discussed.	1. Many of the existing security solution techniques are generating a hefty load in communication and computation for smart devices. Lightweight security and privacy defenses are vulnerable to attacks easily.	1. Device Learning procedures are used to improve this performance of network safety in IoT devices.	To develop an app for security and privacy Challenges in IoT systems.
2	[105]	Syeda Manjia Tahsien et al. & 2020	All types of machine learning techniques explained	1. Existing techniques are not proficient to secure smart technology.	1. IoT is updating devices rapidly with different firmware and software. So, continuous learning is one of the solutions to protect from threats. 2. ML techniques are used to identify the smart attacks on IoT devices with enhanced defensive policy.	Identified limitations and challenges can be used to protect the future IoT network.
3	[106]	Fatima Hussain et al. & 2020	All types of machine learning techniques explained.	1. One of the serious challenges in IoT is botnet attacks. 2. It scans the entire network intelligently and spread the threats. 3. So, traditional cryptographic approaches are insufficient to secure the entire IoT network. 4. Behavioral-based and signature-based traditional techniques fail to identify zero-day intrusions.	1. ML can predict malicious code in IoT applications with more accuracy through continuous learning. 2. ML-based security mechanisms are highly effective and low-cost for smart applications.	Limitations of traditional ML security mechanisms are outlined for future research enhancements
4	[107]	Bhabendu Kumar Mohanta et al. & 2020	All Machine Learning techniques are reviewed.	1. Emerging technology approaches with refuge and secrecy issues. 2. Customary-based protocol refuge methodologies are inappropriate to the current intelligent techniques.	1. ML is one of the leading technologies to secure IoT applications. 2. It is used to make the decisions on smart application security before that event occurs through continuous learning.	An in-depth survey on security challenges and solutions is used to implement s the IoT applications securely.

5	[108]	José Roldán et al. & 2020	Support Vector Regression (SVR), Complex Event Processing (CEP)	1. Increases in the smart environment are to bring many threats and attacks on cyber security. 2. It includes DoS attacks, malware, and privacy breaches in IoT applications.	1. This technique is used to detect the different types of attacks in real-time applications. 2. MEdit4CEP tool is used to correlate and analyze the entire IoT network to detect and prevent attacks in real-time applications.	To identify more attack patterns on IoT technology by using automatic predictors with required training.

real-world smart applications are implemented using IoT technology to change our environments into smart ones. In this world, communication between devices is possible anywhere and anytime without human intervention. These connected devices collect and transfer more information to improve the quality of human life through wireless technology. It comes with more challenging issues, like security breaches and privacy attacks on objects. In IoT technology, security and privacy play a vital role, and traditional solution techniques suffer from complex issues and novel hacking procedures. As an IoT applications and device developers, we need to consider these kinds of security problems when delivering secured products to end-users. Periodically, we need to reevaluate the security intimidations, architectures, software & access codes on smart applications. In this paper, a complete review of the IoT infrastructure is presented, which also includes enabling technologies, enhanced architectures, secrecy, privacy risks, and solutions. In this work, we elaborate on existing techniques based on security and privacy attacks and controls in the layered architecture of the IoT to fulfill the concerns by using a bio-inspired optimization model for better accuracy in attack detection. Bio-inspired optimization (BIO) trained model is presented towards defending the security and privacy of patient confidential data that are transmitted transversely to the smart connected healthcare applications. This will provide a better understanding of the issues of the smart application to consumers and researchers for future directions. Future, the plan is to develop a new enhanced learning-based bio-inspired optimization algorithm for IoT security and privacy problems in real-time applications.

References

[1] A. Salam, "Internet of things for sustainable community development: introduction and overview," in *Internet of Things for Sustainable Community Development*. Springer, 2020, pp. 1–31.

[2] M. Adegboye, O. Olaniyan, O. Okwor, L. Ajao *et al.*, "Internet of things: survey of the security challenges and countermeasures," 2016.

[3] C. Li and B. Palanisamy, "Privacy in internet of things: From principles to technologies," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488–505, 2018.

[4] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "Iot elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, 2018.

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE internet of things journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[6] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[7] M. Bansal, M. Nanda, and M. N. Husain, "Security and privacy aspects for internet of things (iot)," in *2021 6th International Conference on Inventive Computation Technologies (ICICT)*. IEEE, 2021, pp. 199–204.

[8] X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang, H. Sun, and C. Huang, "Secure identity authentication of community medical internet of things," *IEEE Access*, vol. 7, pp. 115 966–115 977, 2019.

[9] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567–3569, 2018.

[10] X. Guo, J. Hua, Y. Zhang, and D. Wang, "A complexity-reduced block encryption algorithm suitable for internet of things," *IEEE Access*, vol. 7, pp. 54 760–54 769, 2019.

[11] H. Cui, R. H. Deng, J. K. Liu, X. Yi, and Y. Li, "Server-aided attribute-based signature with revocation for resource-constrained industrial-internet-of-things devices," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3724–3732, 2018.

[12] S. Roy, U. Rawat, and J. Karjee, "A lightweight cellular automata based encryption technique for iot applications," *IEEE Access*, vol. 7, pp. 39 782–39 793, 2019.

[13] K. Saleem, J. Chaudhry, M. A. Orgun, and J. Al-Muhtadi, "A bio-inspired secure ipv6 communication protocol for internet of

things," in *2017 Eleventh International Conference on Sensing Technology (ICST)*. IEEE, 2017, pp. 1–6.

[14] N. Hitaswi and K. Chandrasekaran, "A bio-inspired model to provide data security in cloud storage," in *2016 International Conference on Information Technology (InCITe)-The Next Generation IT Summit on the Theme-Internet of Things: Connect your Worlds*. IEEE, 2016, pp. 203–208.

[15] C. O. Muango, J. O. Malenje, and Q. Shaojian, "Bio-inspired security scheme for iot technology," *International Journal of Computer Applications*, vol. 975, p. 8887.

[16] S. Aldhaheri, D. Alghazzawi, L. Cheng, A. Barnawi, and B. A. Alzahrani, "Artificial immune systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research," *Journal of Network and Computer Applications*, vol. 157, p. 102537, 2020.

[17] Z. Amjad, M. A. Shah, C. Maple, H. A. Khattak, Z. Ameer, M. N. Asghar, and S. Mussadiq, "Towards energy efficient smart grids using bio-inspired scheduling techniques," *IEEE Access*, vol. 8, pp. 158 947–158 960, 2020.

[18] U. Rauf, "Bio-inspired cyber security and threat analytics," Ph.D. dissertation, The University of North Carolina at Charlotte, 2020.

[19] I. Dumitrache, S. I. Caramihai, I. S. Sacala, M. A. Moisescu, and D. C. Popescu, "Future enterprise as an intelligent cyber-physical system," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 10 873–10 878, 2020.

[20] M. F. A. Razak, N. B. Anuar, F. Othman, A. Firdaus, F. Afifi, and R. Salleh, "Bio-inspired for features optimization and malware detection," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 6963–6979, 2018.

[21] A. O. de Sá, L. F. d. C. Carmo, and R. Machado, "Bio-inspired active system identification: a cyber-physical intelligence attack in networked control systems," *Mobile Networks and Applications*, vol. 25, no. 5, pp. 1944–1957, 2020.

[22] P. Nespoli, F. G. Mármol, and J. M. Vidal, "A bio-inspired reaction against cyberattacks: Ais-powered optimal countermeasures selection," *IEEE Access*, vol. 9, pp. 60 971–60 996, 2021.

[23] N. Hosseini, F. Fakhar, B. Kiani, and S. Eslami, "Enhancing the security of patients' portals and websites by detecting malicious web crawlers using machine learning techniques," *International journal of medical informatics*, vol. 132, p. 103976, 2019.

[24] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, and Y. Liu, "A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 3–12, 2018.

[25] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in iot sensors in iot sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019.

[26] Z. Rayan, M. Alfonse, and A.-B. M. Salem, "Machine learning approaches in smart health," *Procedia Computer Science*, vol. 154, pp. 361–368, 2019.

[27] A. Mathews, "What can machine learning do for information security?" *Network Security*, vol. 2019, no. 4, pp. 15–17, 2019.

[28] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice," *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, 2018.

[29] T. Malche and P. Maheshwary, "Internet of things (iot) for building smart home system," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 65–70.

[30] W. A. Jabbar, T. K. Kian, R. M. Ramli, S. N. Zubir, N. S. Zamrizaman, M. Balfaqih, V. Shepelev, and S. Alharbi, "Design and fabrication of smart home with internet of things enabled automation system," *IEEE access*, vol. 7, pp. 144 059–144 074, 2019.

[31] N. Mohamed, J. Al-Jaroodi, and S. Lazarova-Molnar, "Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories," *Ieee Access*, vol. 7, pp. 18 008–18 020, 2019.

[32] Sales, "8 uses," *Applications, and Benefits of Industrial IoT in Manufacturing [Blog post]. (2017, December*, 2017.

[33] R. K. Pathinarupothi, P. Durga, and E. S. Rangan, "Iot-based smart edge for global health: Remote monitoring with severity detection and alerts transmission," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2449–2462, 2018.

[34] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in iot," *IEEE Access*, vol. 7, pp. 135 632–135 649, 2019.

[35] A. Alabdulatif, I. Khalil, X. Yi, and M. Guizani, "Secure edge of things for smart healthcare surveillance framework," *IEEE Access*, vol. 7, pp. 31 010–31 021, 2019.

[36] A. Ahad, M. Tahir, and K.-L. A. Yau, "5g-based smart healthcare network: architecture, taxonomy, challenges and future research directions," *IEEE access*, vol. 7, pp. 100 747–100 762, 2019.

[37] H. Qiu, M. Qiu, and Z. Lu, "Selective encryption on ecg data in body sensor network based on supervised machine learning," *Information Fusion*, vol. 55, pp. 59–67, 2020.

[38] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe, and A. Welhenge, "Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions," *Sustainability*, vol. 13, no. 21, p. 11645, 2021.

[39] Q. Ha and M. D. Phung, "Iot-enabled dependable control for solar energy harvesting in smart buildings," *IET Smart Cities*, vol. 1, no. 2, pp. 61–70, 2019.

[40] F. M. Bhutta, "Application of smart energy technologies in building sector—future prospects," in *2017 International Conference on Energy Conservation and Efficiency (ICECE)*. IEEE, 2017, pp. 7–10.

[41] N. Havard, S. McGrath, C. Flanagan, and C. MacNamee, "Smart building based on internet of things technology," in *2018 12th International conference on sensing technology (ICST)*. IEEE, 2018, pp. 278–281.

[42] A. Llaria, J. Dos Santos, G. Terrasson, Z. Boussaada, C. Merlo, and O. Curea, "Intelligent buildings in smart grids: A survey

on security and privacy issues related to energy management," *Energies*, vol. 14, no. 9, p. 2733, 2021.

[43] Z. Hu, L. Xu, L. Cao, S. Liu, Z. Luo, J. Wang, X. Li, and L. Wang, "Application of non-orthogonal multiple access in wireless sensor networks for smart agriculture," *IEEE Access*, vol. 7, pp. 87 582–87 592, 2019.

[44] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A survey on the role of iot in agriculture for the implementation of smart farming," *Ieee Access*, vol. 7, pp. 156 237–156 271, 2019.

[45] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-things (iot)-based smart agriculture: Toward making the fields talk," *IEEE access*, vol. 7, pp. 129 551–129 583, 2019.

[46] V. Javidroozi, H. Shah, and G. Feldman, "Urban computing and smart cities: Towards changing city processes by applying enterprise systems integration practices," *IEEE Access*, vol. 7, pp. 108 023–108 034, 2019.

[47] M. J. Kaur and P. Maheshwari, "Building smart cities applications using iot and cloud-based architectures," in *2016 International Conference on Industrial Informatics and Computer Systems (CIICS)*. IEEE, 2016, pp. 1–5.

[48] R. Du, P. Santi, M. Xiao, A. V. Vasilakos, and C. Fischione, "The sensable city: A survey on the deployment and management for smart city monitoring," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1533–1560, 2018.

[49] M. Rouse, S. Shea, and E. Burns, "Smart city," https://www.techtarget.com/iotagenda/definition/smart-city, https, 2018.

[50] C. Vorakulpipat, R. K. Ko, Q. Li, and A. Meddahi, "Security and privacy in smart cities," 2021.

[51] A. Kumar, A. K. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in rfid," *Complex & Intelligent Systems*, vol. 7, no. 3, pp. 1327–1347, 2021.

[52] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in internet-of-things (iots) framework," *Future generation computer systems*, vol. 108, pp. 909–920, 2020.

[53] R. Jiang, M. Shi, and W. Zhou, "A privacy security risk analysis method for medical big data in urban computing," *IEEE Access*, vol. 7, pp. 143 841–143 854, 2019.

[54] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE communications surveys & tutorials*, vol. 20, no. 1, pp. 566–600, 2017.

[55] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1–44, 2021.

[56] J. C.-W. Lin and K.-H. Yeh, "Security and privacy techniques in iot environment," p. 1, 2020.

[57] A. Al-Gburi, A. Al-Hasnawi, and L. Lilien, "Differentiating security from privacy in internet of things: a survey of selected threats and controls," in *Computer and network security essentials*. Springer, 2018, pp. 153–172.

[58] F. Team, ""iot DoS attacks – how hacked IoT devices can lead to massive denial of service attacks," 2018.

[59] Z. Benenson, F. Gassmann, and R. Landwirth, "Unpacking spear phishing susceptibility," in *International conference on financial cryptography and data security*. Springer, 2017, pp. 610–627.

[60] Q. I. Sarhan, "Internet of things: a survey of challenges and issues," *International Journal of Internet of Things and Cyber-Assurance*, vol. 1, no. 1, pp. 40–75, 2018.

[61] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & iot," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[62] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[63] A. Ahmed, R. Latif, S. Latif, H. Abbas, and F. A. Khan, "Malicious insiders attack in iot based multi-cloud e-healthcare environment: a systematic literature review," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 21 947–21 965, 2018.

[64] D. Mocrii, Y. Chen, and P. Musilek, "Iot-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1, pp. 81–98, 2018.

[65] K. Kumar, "Intrusion detection and prevention system in enhancing security of cloud environment," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 6, no. 8, 2017.

[66] C. Lei, H.-Q. Zhang, J.-L. Tan, Y.-C. Zhang, and X.-H. Liu, "Moving target defense techniques: A survey," *Security and Communication Networks*, vol. 2018, 2018.

[67] T. M. Alfaqih and J. Al-Muhtadi, "Internet of things security based on devices architecture," *International Journal of Computer Applications*, vol. 975, p. 8887, 2016.

[68] Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, "Internet of things and the man-in-the-middle attacks–security and economic risks," *MEST Journal*, vol. 5, no. 2, pp. 15–25, 2017.

[69] C. Renuka Venkata Ramani, "Two way firewall for internet of things," 2016.

[70] B. Cruz, S. Gómez-Meire, D. Ruano-Ordás, H. Janicke, I. Yevseyeva, and J. R. Méndez, "A practical approach to protect iot devices against attacks and compile security incident datasets," *Scientific Programming*, vol. 2019, 2019.

[71] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3496–3509, 2018.

[72] M. F. Elrawy, A. I. Awad, and H. F. Hamed, "Intrusion detection systems for iot-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, pp. 1–20, 2018.

[73] O. A. Okpe, O. A. John, and S. Emmanuel, "Intrusion detection in internet of things (iot)." *International Journal of Advanced Research in Computer Science*, vol. 9, no. 1, 2018.

[74] C. Suchitra and C. Vandana, "Internet of things and security issues," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 1, pp. 133–139, 2016.

[75] A. Haritha and A. Lavanya, "Internet of things: Security issues," *International Journal of Engineering Science Invention ISSN (Online)*, vol. 6, no. 11, 2017.

[76] M. L. Das, P. Kumar, and A. Martin, "Secure and privacy-preserving rfid authentication scheme for internet of things applications," *Wireless Personal Communications*, vol. 110, no. 1, pp. 339–353, 2020.

[77] A. Hezam, D. Konstantas, and M. Mahyoub, "A comprehensive iot attacks survey based on a building-blocked reference mode," *Int. J. Adv. Comput. Sci. Appl*, vol. 9, pp. 355–373, 2018.

[78] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An iot perspective," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 22, 2019.

[79] A. Hassan, "Lightweight cryptography for the internet of things," in *Proceedings of the Future Technologies Conference*. Springer, 2020, pp. 780–795.

[80] L. M. Shamala, G. Zayaraz, K. Vivekanandan, and V. Vijayalakshmi, "Lightweight cryptography algorithms for internet of things enabled networks: An overview," in *Journal of Physics: Conference Series*, vol. 1717, no. 1. IOP Publishing, 2021, p. 012072.

[81] L. Gavoni, "Rfid exploitation and countermeasures," *arXiv preprint arXiv:2110.00094*, 2021.

[82] S. Naaz and M. S. Sajad, "Radio frequency identification [rfid] technology: A studyondawning issues, challenges and future modifications," 2020.

[83] A. W. Ahmed, O. A. Khan, M. A. Mian, and M. A. Shah, "A comprehensive analysis on the security threats and their countermeasures of iot," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, 2017.

[84] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.

[85] J. Chen, "Hybrid blockchain and pseudonymous authentication for secure and trusted iot networks," *ACM SIGBED Review*, vol. 15, no. 5, pp. 22–28, 2018.

[86] P. Zhao, H. Jiang, C. Wang, H. Huang, G. Liu, and Y. Yang, "On the performance of k-anonymity against inference attacks with background information," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 808–819, 2018.

[87] M. Park, H. Oh, and K. Lee, "Security risk measurement for information leakage in iot-based smart homes from a situational awareness perspective," *Sensors*, vol. 19, no. 9, p. 2148, 2019.

[88] R. M. Salih, *Using Agent-Based Implementation of Active Data Bundles for Protecting Privacy in Healthcare Information Systems*. Western Michigan University, 2018.

[89] L. T. Yang, W. Wang, G. M. Perez, and W. Susilo, "Security, privacy, and trust for cyberphysical-social systems," 2019.

[90] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *CoRR*, vol. abs/1807.11023, 2018. [Online]. Available: http://arxiv.org/abs/1807.11023

[91] C. Ramakrishna, G. K. Kumar, A. M. Reddy, and P. Ravi, "A survey on various iot attacks and its countermeasures," *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, vol. 5, no. 4, pp. 143–150, 2018.

[92] Y. Kumar, "Juice jacking-the usb charger scam," *Available at SSRN 3580209*, 2020.

[93] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of things Journal*, vol. 6, no. 2, pp. 1606–1616, 2018.

[94] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, and S. Yu, "Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3492–3500, 2021.

[95] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment," *Future Generation Computer Systems*, vol. 83, pp. 629–637, 2018.

[96] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for internet of things," *Internet of Things*, vol. 14, p. 100075, 2021.

[97] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," *arXiv preprint arXiv:1901.07309*, 2019.

[98] Y. Lu and L. Da Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2018.

[99] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice-based public key cryptosystem for internet of things environment: Challenges and solutions," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4897–4909, 2018.

[100] M. Malik, M. Dutta, and J. Granjal, "A survey of key bootstrapping protocols based on public key cryptography in the internet of things," *IEEE Access*, vol. 7, pp. 27 443–27 464, 2019.

[101] N. Primeau, R. Falcon, R. Abielmona, and E. M. Petriu, "A review of computational intelligence techniques in wireless sensor and actuator networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2822–2854, 2018.

[102] U. Rauf, "A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 6693–6708, 2018.

[103] K. Munivara Prasad, A. Rama Mohan Reddy, and K. Venugopal Rao, "Bifad: Bio-inspired anomaly based http-flood attack detection," *Wireless Personal Communications*, vol. 97, no. 1, pp. 281–308, 2017.

[104] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "Iot security techniques based on machine learning: How do iot devices use ai to enhance security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[105] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (iot): A survey," *Journal of Network and Computer Applications*, vol. 161, p. 102630, 2020.

[106] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.

[107] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020.

[108] J. Roldán, J. Boubeta-Puig, J. L. Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: An intelligent architecture for detecting iot security attacks," *Expert Systems with Applications*, vol. 149, p. 113251, 2020.

[109] M. Golec, R. Ozturac, Z. Pooranian, S. S. Gill, and R. Buyya, "ifaasbus: A security-and privacy-based lightweight framework for serverless computing using iot and machine learning," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3522–3529, 2021.

[110] A. Awad, S. J. Trenfield, T. D. Pollard, J. J. Ong, M. Elbadawi, L. E. McCoubrey, A. Goyanes, S. Gaisford, and A. W. Basit, "Connected healthcare: Improving patient care using digital health technologies," *Advanced Drug Delivery Reviews*, vol. 178, p. 113958, 2021.

[111] S. M. Karunarathne, N. Saxena, and M. K. Khan, "Security and privacy in iot smart healthcare," *IEEE Internet Computing*, vol. 25, no. 4, pp. 37–48, 2021.

[112] A. N. Navaz, M. A. Serhani, H. T. El Kassabi, N. Al-Qirim, and H. Ismail, "Trends, technologies, and key challenges in smart and connected healthcare," *Ieee Access*, vol. 9, pp. 74 044–74 067, 2021.

[113] M. N. Alraja, H. Barhamgi, A. Rattrout, and M. Barhamgi, "An integrated framework for privacy protection in iot—applied to smart healthcare," *Computers & Electrical Engineering*, vol. 91, p. 107060, 2021.

[114] J. Hu, W. Liang, O. Hosam, M.-Y. Hsieh, and X. Su, "5gss: A framework for 5g-secure-smart healthcare monitoring," *Connection Science*, vol. 34, no. 1, pp. 139–161, 2022.

[115] Y. Ould-Yahia, S. Banerjee, S. Bouzefrane, and H. Boucheneb, "Exploring formal strategy framework for the security in iot towards e-health context using computational intelligence," in *Internet of things and Big data technologies for next generation healthcare*. Springer, 2017, pp. 63–90.

[116] M. Cococcioni, "Computational intelligence in maritime security and defense: Challenges and opportunities," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2018, pp. 1964–1967.

Author 1 Sripriyanka G Sripriyanka G has done her B.Sc Computer Science from Vellore Institute of Technology, Vellore, India in 2013, M.Sc Computer Science from Vellore Institute of Technology, Vellore, India in 2016, M.Tech (Computer Science and Engineering) from Vellore Institute of Technology, Vellore, India in 2018 and Currently, she is doing Ph.D. in Computer Science and Engineering from Vellore Institute of Technology, Vellore, India. Her research interests include Internet of Things, security and bio-inspired computing techniques.

Author 2 Anand Mahendran Anand Mahendran received his Ph.D. (Computer Science and Engineering) from Vellore Institute of Technology, Vellore, India, in 2012, M.E. (Computer Science and Engineering) from Anna University, India, in 2005, and B.E. (Computer Science and Engineering) from Vellore Institute of Technology, Vellore, India, in 2003. His research interests include formal language theory and automata, and bio-inspired computing models. He has published more than 50 papers in international journals and refereed international conferences. Currently, he is doing his Post-Doc in Laboratory of Theoretical Computer Science, National Research University, Higher School of Economics, Moscow, Russia.