e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712123

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey

Arsh Singh, Dr. Anita Choudhary

Student, NIMS School of Business Studies, NIMS University, Jaipur, India

Assistant Professor, NIMS School of Business Studies, NIMS University, Jaipur, India

ABSTRACT: Through three development routes of authentication, communication, and computing, the Inter- net of Things (IoT) has become a variety of innovative integrated solutions for specific applications. However, due to the openness, extensiveness and resource constraints of IoT, each layer of the three-tier IoT architecture suffers from a variety of security threats. In this work, we systematically review the particularity and complexity of IoT security protection, and then find that Artificial Intelligence (AI) methods such as Machine Learning (ML) and Deep Learning (DL) can provide new powerful capabilities to meet the security requirements of IoT. We analyze the technical feasibility of AI in solving IoT security problems and summarize a general process of AI solutions for IoT security. For four serious IoT security threats: device authentication, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks defense, intrusion detection and malware detection, we summarize representative AI solutions and compare the different algorithms and technologies used by various solutions. It should be noted that although AI provides many new capabilities for the security protection of IoT, it also brings new potential challenges and possible negative effects to IoT in terms of data, algorithm and architecture. In the future, how to solve these challenges can serve as potential research directions.

KEY WORSDS: Artificial intelligence, deep learning, Internet of Things, machine learning, security.

I.INTRODUCTION

The International Telecommunication Union formally pro- posed the concept of ‘‘Internet of Things’’ at the World Summit on the Information Society (WSIS) in 2005 [1]. The Internet of things (IoT) refers to a distributed network that combines various sensor devices and systems, such as sen- sor networks, RFID devices, barcode and QR code devices, global positioning systems, etc. [2], with the Internet through wired and wireless communication technologies, enabling embedded systems to communicate and interconnect.
From the discovery of electromagnetic induction to RFID, from simple sensors to ubiquitous connections, from elec- tronic toll collection (ETC) to smart cities, the development of IoT has always been along the following three technical routes:

authentication technologies are the foundation of IoT. As nerve endings of IoT, sensors are the largest and most basic part of the chain of IoT. A large number of general-purpose sensor devices have been popularized, and high-end sensor devices in specific fields have also made great progress.

The development of transmission and communication technologies. Transmission and communication t eoch- nologies are the guarantee of IoT. The large amount of information collected by IoT devices needs be transmitted and aggregated to the central node or the processing unit in a more convenient, more reliable, and safer way. The development of wired and wireless networks, cellular networks, and other transmission and communication technologies have made it possible for large-scale IoT data transmission.

The development of data computing and processing technologies. Data computing and processing tech- nologies are essential to provide applications and ser- vices using IoT data. IoT applications need real- time non-cellular networks (ZigBee, Bluetooth and Wi-Fi, etc.) and cellular networks (NB-IoT, eMTC, etc.)

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

for data encoding, authentication, and transmission. The application service layer processes the data transmit- ted from the network transport layer and integrates them with various industries to support vertical applications of IoT, pro- viding rich and specific services for different users in specific fields, such as smart grids, smart homes, and smart cities. The application service layer also includes application & service subsystems that provide capabilities of data storage, analysis and service, as well as operation maintenance & manage- ment subsystems that provide capabilities of management and operation support.

II.IOT SECURITY THREATS

As more and more machines and smart devices are connected to the network, the vulnerabilities of IoT security are gradu- ally exposed. IoT devices are more vulnerable to be attacked than computers or mobile phones, not only because of the surge in the use of IoT devices, but also on account of the complexity, diversity, and inherent mobility of such device application scenarios. At the same time, IoT has developed rapidly but has not yet matured. The privacy protection crises caused by the openness of the network and the mobility of data are less discussed and regulated.
Comprehensive per- ception makes the data collected and exchanged by IoT more private and dangerous than the Internet.

A.ATTRIBUTION ANALYSIS OF IoT SECURITY
The widespread popularity and the large-scale deployment have promoted the development of IoT, but also brought new security challenges. Maintaining its security is a complex and challenging task. The reasons for the increasingly serious security problems of IoT are as follows:

The lack of human supervision. IoT terminals are usually deployed in complex and changeable environments to col- lect information and provide data for applications. However, under these environmental conditions, due to the limitation of human resources, the terminals are exposed, distributed and unattended, so that intruders can easily physically damage devices [5]. Common physical attacks include illegal theft, malicious movement, etc. These attacks will cause damage, data loss and function failure of IoT devices. In the case of huge amount of IoT devices, it is difficult to find and repair damaged terminals in time, which further aggravates the consequences of physical attacks.
The resource constraints of low-power devices and terminals. IoT devices are small in size and low in power consumption. They can do some simple data calculations and are suitable for distributed computing. In recent years, the rapid development of edge computing takes advantage of this characteristic of IoT devices [6]. However, the limited computing capacity and power supply cannot support a large number of complex calculations. There are no remaining resources to implement more fine-grained security measures, resulting in the inability of IoT devices and systems to use complex security mechanisms [7]. The use of some measures may reduce the equipment processing efficiency and increase resource consumption, thus causing damage to the original services. For example, RSA, a commonly used encryption protocol, will consume a lot of resources when running on devices with

2)THERE ARE RISKS OF BEING ATTACKED DURING THE INFORMATION TRANSMISSION OF IoT NODES
There are three main types of terminal perception layer nodes: collection endpoints, information aggregation nodes, and iso- lated nodes. The collection endpoint mainly corresponds to sensors, which is responsible for sensing and collecting information; the information aggregation node is the server responsible for receiving, processing, forwarding informa- tion; the isolation node is embedded equipment responsible for the operations of information encryption and decryption, internal and external network isolation. When information is interconnected between nodes, due to the transmission dis- tance, there are threats such as interception, eavesdropping, counterfeiting, and tampering of nodes.

3)THE IDENTIFICATION AND AUTHENTICATION TECHNOLOGIES ARE INDISPENSABLE PREREQUISITES FOR THE
SECURE COMMUNICATION OF IoT DEVICES [10] Although the uniqueness and certainty of identity can effec- tively increase the security of IoT devices, hackers can use some ways to bypass this process to
implement intrusion. For example, in April 2019, a software called iLnkP2P was dis- covered without any authentication or encryption measures. Attackers can bypass the firewall with some specific serial numbers and directly establish connections with IoT devices, send malicious messages instead of any valid messages sent by the device.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. SECURITY THREATS IN THE NETWORK TRANSPORT LAYER

IoT integrates sensor networks [11] and communication net- works to form a large-scale network. Similar to the risks faced by the terminal perception layer, the possible attacks also increase significantly with the increase of network scale.

1)THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF NETWORK ARE TARGETS OF NETWORK TRANSPORT LAYER'S ATTACKERS [12]

Some network targets have poor protection, which makes it easier for attackers to invade. When the system lacks protection and verification mechanisms, the attacker will tamper with the platform software and hardware modules, resulting in the risk of leakage of stored information. Therefore, timely detection of intrusions is critical to curb attacks and protect network security in the early stages.

2)NETWORK TRANSPORT LAYER WILL SUFFER FROM ATTACKS SUCH AS DENIAL OF SERVICE (DoS) AND DISTRIBUTED DENIAL OF SERVICE (DDoS)

Attackers launch DoS and DDoS attacks by sending traffic beyond the target's processing capacity to consume computing and network resources of the target, resulting in resource depletion, thus blocking the target network and causing denial of service. Large-scale DoS and DDoS attacks will cause dis- astrous consequences to the whole network. Mirai, the botnet
which broke out in 2016, launched a large-scale DDoS attack by using IoT devices, resulting in more than 100,000 devices infected [13].

3)THE COMMUNICATION TECHNOLOGIES USED BY IoT HAVE LIMITATIONS

IoT uses different communication technologies [14], includ- ing long-distance networks (NB-IoT and LoRa (Long Range Radio) [15]), short-distance networks (ZigBee [16], Wi-Fi, etc.), and Internet. The security shortcomings of these technologies have been inherited into IoT. For example, the Internet provides a wide range of services for different participants, including IoT users, but at the same time, the communication infrastructure based on TCP / IP is not only vulnerable to security and privacy threats,

1)SYSTEM SECURITY

The application service layer usually consists of basic envi- ronments, components, and virtualized cloud platforms. Basic environments and components, such as operating sys- tems, databases and middleware, will be used by attackers to launch brute force attacks and man-in-the-middle attacks, resulting in unauthorized access, remote control and data leakage. Most IoT systems build virtualized cloud platforms to reduce equipment deployment costs and improve computing performance or business throughput.
However, vir- tualization technology also brings security risks, leading to blurring of the boundary between users and data, resulting in security issues including virtual machine escape, virtual network attacks, and virtualized software vulnerabilities.

2)DATA SECURITY

Databases face security problems. Common database attacks include SQL injection [19], privilege promotion and backup theft. Data privacy protection is an important security require- ment of the application service layer. Many information obtained by the IoT may contain personal privacy, such as positioning information obtained by GPS. Such information can be used by attackers to analyze users' sensitive privacy such as residence, income, lifestyle, behavior, and health status [20].

3)SOFTWARE SECURITY

Malicious applications are commonly used by software attackers. For example, in 2017, Bank of Russia found a malware called Bespalova existed in ATMs, which automatically paid after entering a specific code. If the system does not have enough code checks and tests, it will be vulnerable to attacks by malicious scripts or error indications. For example, attackers will use XSS (Cross-Site Scripting Attack)

[21] to inject some malicious scripts into another trusted website. Successful XSS attacks can lead to hijacking IoT accounts and paralyzing the IoT system. In addition, Android malware has increased significantly in recent years [22].

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

For mobile devices, the openness of the Android mobile operating system has contributed to the spread of malware. Malware can use vulnerabilities to invade users' mobile phones and obtain private data.

III.FEASIBILITY ANALYSIS OF APPLYING AI IN IOT SECURITY A. COMMON CHARACTERISTICS AND SPECIAL REQUIREMENTS OF IOT SECURITY

Through the analysis of various security problems faced by IoT, it can be found that IoT security problems have some common characteristics which makes IoT security more complex and produces special requirements for security pro- tection that are different from other fields.

1)THE INTEGRITY OF IoT REQUIRES THAT SECURITY SCHEMES CAN EFFECTIVELY HANDLE MASSIVE DATA AND

CAN be and service platforms, the defense of security issues is holistic and data are more complex and large-
s ce ac luer.i tTyh e unity and integrity of IoT put forward an urgent demand for the process- ing capacity of solutions under massive data, and it is necessary to ensure that solutions can be uniformly deployed in a large-scale way, remain effective in complex situations, and can evolve according to new scenarios at any time.

A. NEW CAPABILITIES PROVIDED BY AI TO IoT SECURITY
The particularity of IoT security and limitations of traditional methods highlight the urgent need for new security technolo- gies. As a new technology direction, artificial intelligence has a wide range of applicability [26]. Machine learning (ML) is a research focus in the field of artificial intelligence. Its theory and methods have been widely used to solve complex problems in many engineering applications. The ML algorithms applied to IoT security can be divided into transaction algorithms and decision algorithms.

2). Transaction algorithms are mainly responsible for data exploration and data preprocessing.
use few samples and simple models to obtain the general characteristics of the dataset and provide the basis for deci- sion algorithms. Decision algorithms are mainly responsible for business decisions and adopt different decision-making strategies to reduce the ratio of misjudgment, so that the over- all profit is the highest. Decision algorithms can be divided into three types according to strategies and scenarios: single decision-making, sequential decision-making, and integrated decision-making.

In addition, machine learning methods can be divided more carefully (as shown in Table 1), including Supervised Learning [27], Unsupervised Learning [28], Reinforcement Learning (RL) [29], Ensemble Learning [30], and Deep Learning (DL) [31]. Machine learning can make up for the defects of traditional security solutions in different aspects, conform to the charac- teristics of IoT and provide new capabilities for IoT to meet the new security requirements mentioned above. environment, maintain the validity, and strengthen the active exploration ability of the model, thus laying the foundation for the realization of active immunity of IoT security.

3) THE CAPABILITY OF PROCESSING LARGE AMOUNTS OF COMPLEX DATA EFFECTIVELY
Traditional IoT security schemes usually work under the limited amount of data. With the increasing generation of data, the deficiencies of these schemes in big data process- ing capacity and computing efficiency are highlighted. For example, malware detection is the primary task of software security in application service layer. Traditional malware detection methods extract malicious behavior codes from malware as signatures, and judge whether a new software is malware by calculating the similarity between the software to be detected and the signature database. When the amount and dimensions of data increase, the computational complexity will rise rapidly, resulting in the efficiency of the model is greatly reduced, and it is unable to make timely and effective detection. Compared with traditional schemes, the advantage of AI schemes is that it can not only process small- scale data, adding or deleting nonsupport vector samples has no effect on the model, which makes SVM have good robustness; random forest has good anti-noise ability and is insensitive to outliers; linear models with L1 and L2 regularization [40] has excellent generalization ability and can avoid over-fitting. These ML methods with good robustness and generalization ability can greatly enhance the applicability and scalability of IoT security solutions.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV.AI SOLUTIONS TO FOUR IOT SECURITY THREATS

A.FOUR THREATS TO IoT SECURITY

According to investigation, there are four threats that need to be solved urgently in IoT security: device authentication, DoS/DDoS attack, intrusion detection, and malware detec- tion. The traditional solutions to these problems lack the processing ability of large data sets and have many problems such as low efficiency and poor real-time performance. Most of them cannot be migrated to IoT. AI methods represented by machine learning can use massive IoT data to infer useful knowledge from the data, and thus make predictions for unknown events, providing new solutions for these problems.

1)DEVICE AUTHENTICATION

There are risks of interception, counterfeiting, tampering, and destruction in the process of information interaction and data transmission between IoT nodes. In order to prevent the transmission of false information, the security requirements between nodes include identity authentication, judgment and blocking malicious nodes [50]. The authentication process of IoT devices is generally restricted by the characteristics of the IoT, such as limited resources. Therefore, it is necessary to ensure that the calculation and communication cost do not exceed the limitations of the device as much as possi- ble, to ensure that the device does not consume too many resources [50].

2)DoS / DDoS ATTACK

Denial-of-service attacks (DoS) [51] and distributed denial- of-service attacks (DDoS) [52] use weaknesses in the trans- mission protocol, or vulnerabilities in systems and servers to launch large-scale destructive attacks on the target system. Massive data packets exceeding the target processing capac- ity will consume available network bandwidth resources, causing program buffer overflow, preventing other legitimate users from normal requests, and ultimately lead to network service paralysis or system crash. There are some differences between DDoS and DoS. DDoS uses multiple distributed attackers in different positions to launch attacks on one or several targets at the same time, or an attacker controls mul- tiple machines in different positions and uses these machines to attack the victim.

3)INTRUSION DETECTION [53]

Intrusion Detection aims to monitor events that occur in the system, by collecting and analyzing the information of key points, to check whether there are behaviors that violate the security policy to achieve early detection of intrusion. As an active security protection technology, intrusion detection is an important part of network
security providing real-time protection against internal and external attacks. The ability to detect intrusions and malicious activities in the IoT network is critical to the timely recovery of network infrastructure.

4)MALWARE DETECTION [54]

IoT allows a large number of smart devices to connect to each other to share information and improve the user experience. In order to provide interactive services with users, more and more PC or mobile applications appear. Using vulnerabilities of these applications to inject and execute malicious code in IoT software is a common attack method. These vulnerabil- ities that can be used for malware injection may be related to the authentication and authorization of the application. Physically tampering with IoT devices, software modifica- tions and misconfiguration of security parameters may also allow attackers to inject malicious code. Common malware includes bots, ransomware, adware, etc.

B.GENERAL PROCESS OF AI SOLUTIONS FOR IoT SECURITY

The main tasks of device authentication, DoS / DDoS attack detection, intrusion detection, and malware detection are classification tasks. For example, for device authentication, AI solutions need to be able to accurately classify authorized and unauthorized devices; for intrusion detection, the solu- tions need to be able to classify normal and abnormal network behaviors; and so on. We analyze existing machine learning solutions to these problems and summarize the flow of most solutions into the basic process

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C.AI FOR DEVICE AUTHENTICATION

1)TRADITIONAL DEVICE AUTHENTICATION: DIGITAL CERTIFICATE AUTHENTICATION AND PASSWORD AUTHENTICATION

Digital certificates include user identity information, rely- ing on a trusted third-party Certification Authority (CA) to achieve authentication, and users can access servers of CA with the authentication certificate. The International Telecommunication Union's X.509 standard defines a frame- work for providing authentication services. General CA dig- ital certificates follow X. 509 standard format, so it is also called X. 509 certificate [59]. The password authentication saves the user's name and password in advance [60]. When the user enters the system, the entered information is com- pared with the previously saved information to verify whether the user's identity is legal.

Traditional authentication technologies have many prob- lems. For example, although the password authentication is simple and easy to implement, it is generally only suitable for closed systems. Every time users access the system, they must enter the password in plaintext, which may be intercepted in the process of transmission, thus revealing the privacy infor- mation. Traditional IoT terminals are easy to be counterfeited because of the static nature of identification information [61]. The static of device ID or user ID makes the identity easy to be scanned, read and counterfeited by hackers. ML provide a variety of feasible ideas for secure authentication of IoT. These schemes use a variety of ways to obtain verifiable information related to devices and users. We select several representative schemes for comparative analysis

2)MANUALLY SET INFORMATION: WHITE LIST OR BLACK LIST

The white list and black list are manually set safety / danger- ous device lists, which are often used to screen and intercept connected devices. The goal of device authentication is to ensure that only authorized IoT devices can connect to the network, but there are too many and increasing devices with vulnerabilities, which makes organizations be cautious and skeptical about all IoT devices. A white list of authorized devices will be much smaller than a black list of increas- ing potentially dangerous devices and can also improve the efficiency of ML model training, testing, and deployment. Meidan et al. [62] designed an authentication scheme com- bining white list and ensemble learning, using random forest to perform feature extraction and devices classification of network traffic data in large enterprises IoT. For testing, the average accuracy of the nine device types tested was 99%, and the method was desirable in accuracy and speed of classification.

3)HUMAN BIOLOGICAL CHARACTERISTICS

Human biological characteristics refer to the inherent char- acteristics of the human body such as fingerprints, irises, faces, DNAs, sounds, and so on. Sound sensors in wearable IoT devices such as smartphones and watches can be used for identity authentication. These devices often interact with individuals frequently to obtain personal-specific informa- tion and have unique advantages in fine- grained monitor- ing of user environments. Breath Print is an authentication technology for respiratory acoustics on mobile IoT devices. Breath Print assumes that each person's breathing pattern is unique, thereby taking advantage of the user's respiratory acoustic characteristics captured by wearable IoT devices to support user authentication. With the unique advantages of RNN in audio and speech processing, Chauhan et al. [63] combined RNN with Breath Print to model the collected respiratory acoustic data to distinguish different users. Exper- iments showed that this method can be effectively

4)HUMAN BEHAVIOR CHARACTERISTICS

Human behavior characteristics such as gaits, handwritings, object manipulation habits are also commonly used iden- tity authentication information. Electronic devices in the indoor environment (such as smart refrigerators, smart TVs, smart air conditioners, and security doors) can obtain human behavior characteristics. There are rich Wi-Fi sig- nals between these devices. When operating these devices (such as opening refrigerator doors, entering or leaving room), it is possible to capture the unique physiological and behavioral characteristics of human daily activities, provid- ing a feasible direction for distinguishing each individual. Recognizing user activities needs to start from simple actions and rise to the unique behaviors of different users. The system needs to have abstract capabilities with different granularities, which can extract different levels of feature representation. The powerful abstract representation capa- bilities of deep learning provide the possibility for this. Shi et al. [65] used the amplitude and relative phase of the Channel State Information (CSI) in Wi-Fi signals of house- hold appliances to extract representative human behavior features, combined with the three-hidden-layer DNN model to abstract the features at different levels (Fig. 6). This

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

method achieved the authentication accuracy of 94% and 91% for dynamic and static human activity identification, which proved the feasibility of the combination of Wi-Fi signals and DL.

D. AI FOR DoS/DDoS ATTACK DETECTION AND DEFENSE

L models are always specific to a certain field. When a good model is obtained for a scene and transferred to other similar problems, the original model parameters may fail. We need to retrain new models to replace the original one. For IoT, the diversification of applications will correspond to many different models, all of which need to be maintained and updated. But the process of retraining is cumbersome, there will be many unknown errors, resulting in a huge waste of time and computing resources.

2) INSTABILITY [93] In ML and DL, small changes in the input may cause different effects on the output. Even if the input data of models changes

V. CONCLUSION

The research of this article proves that AI is feasible for the security of IoT, especially for the four key risks: device authentication, DoS / DDoS attack defense, intrusion detec- tion and malware detection. The general process of the AI schemes proposed by us can also be used as a reference to solve IoT security problems in the future. In addition, when AI is applied for IoT security, potential challenges in data, algorithm and architecture need to be solved to avoid adding new threats to IoT security. How to solve these challenges can serve as potential future research directions.

ACKNOWLEDGMENT

(Hui Wu and Haiting Han contribute equally to this work.)

REFERENCES

[1]ITU Internet Reports 2005: The Internet of Things, Geneva, Switzerland: International Telecommunication Union, 2005.

[2]C. Hai-ming, ‘‘Key Technologies and Applications of Internet of Things,’’ Comput. Sci., vol. 36, no. 6, pp. 1–4, 2010.

[3]C.-L. Zhong, Z. Zhu, and R.-G. Huang, ‘‘Study on the IOT architecture and gateway technology,’’ in Proc. 14th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci. (DCABES), Aug. 2015, pp. 196–199, doi: 10.1109/ DCABES.2015.56.

[4]M. Bauer, M. Boussard, N. Bui, J. D. Loof, C. Magerkurth, S. Meiss- ner, A. Nettsträter, J. Stefa, M. Thoma, and J. W. Walewski, ‘‘IoT ref- erence architecture,’’ in Enabling Things to Talk, 2013, pp. 163–211, doi: 10.1007/978-3-642-40403-0_8.

[5]J. Deogirikar and A. Vidhate, ‘‘Security attacks in IoT: A survey,’’ in Proc. Int. Conf., Feb. 2017, pp. 32–37.

[6]W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, ‘‘Edge computing: Vision and challenges,’’ IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[7]E. Bertino, ‘‘Data security and privacy in the IoT,’’ in Proc. EDBT, 2016,
pp. 1–3.

[8]A. Singla, A. Mudgerikar, I. Papapanagiotou, and A. A. Yavuz, ‘‘HAA: hardware-accelerated authentication for Internet of Things in mission critical vehicular networks,’’ in Proc. MILCOM - IEEE Mil. Commun. Conf., Oct. 2015, pp. 1298–1304, doi: 10.1109/MILCOM.2015.7357624.

[9]Cyber Security for Consumer Internet of Things, document TS 103 645, ETSI, 2019.

[10]W. U. Chuankun, L. Zhang, and L. I. Jiangli, ‘‘Design of trust architecture and lightweight authentication scheme for IoT devices,’’ Netinfo Secur., vol. 17, no. 9, pp. 16–20, Oct. 2017.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com