A Review on Security and Privacy Issues in Internet of Things

Amit Kumar Tyagi, Kavita Agarwal, Deepti Goyal and N. Sreenath

Abstract In India, building smart cities is most necessary project for current government, with respect to the getting the status of developed country. But, smart cities are not just built in months, they took years to build because several components need to work together perfectly (which are comes under an ecosystem). To fulfil such goal/smart cities, Internet of Things is mostly used devices to communication with other Internet-connected devices or to do necessary task (for smart city). In near future, most of the things (around the world) will be connected with technology, for example, smart homes, smart cities, smart transportation systems, smart grids, etc., are the applications of advancement in technology (due to integration of Internet of Things together). But, connecting of Internet of Things (IoTs) devices together raised several critical issues like security, privacy, and trust in an ecosystem. In general, Internet of Things (IoTs) are the devices which are connected to do other devices and communicating through sensors and Radio-Frequency Identification (RFID) tags (in the physical world), also through Internet infrastructure. Such issues and challenges need to be listed/investigated for future research. Hence, this article identifies such issues and discusses all of them in detail (from every possible point of view). Together this, this paper also discusses the several benefits or applications of Internet of Things in detail.

Keywords Internet of things · Security · Privacy · Smart things · IoTs applications

A. K. Tyagi (✉) · K. Agarwal · D. Goyal
Department of Computer Science and Engineering, Lingaya's Vidyapeeth, Faridabad 121002, Haryana, India
e-mail: amitkrtyagi025@gmail.com

K. Agarwal
e-mail: goel.kavita15@gmail.com

D. Goyal
e-mail: deeptigoyal1994@gmail.com

N. Sreenath
Pondicherry Engineering College, Puducherry 605014, India
e-mail: nsreenath@pec.edu

H. Sharma et al. (eds.), *Advances in Computing and Intelligent Systems*,
Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-15-0222-4_46

1 Introduction—Internet of Things

Internet of Things is 'a world in which all electronic devices (smart devices) are networked and every object, whether it is physical or electronic, is electronically tagged with information pertinent to that object'. Note that 'Internet of Things' term was first time coined by the cofounder and Executive Director of MIT's Auto-ID lab, Kevin Ashton in the mid-1990s [1]. Several technologies drive the IoT's vision. This is the age of all pervasive connectivity—the 'Internet of Things' (abbreviated as IoT). With the rise of connected devices (with Internet of Things) and connected individuals (systems/devices with sensor), we received combination of four terms (i.e. big data, cloud, social media, and mobile devices and things) or technologies (technology pillars) which works as fuel to industries and helps IoTs to reshape, which has been discussed in [2]. In technical words, connecting devices/things with Internet used three main technology components (i.e. physical devices with sensors/connected things, connection and infrastructure, and analytics and applications), which can be included as follows:

- Physical devices and sensors: They (IoTs) gather and sense multidimensional information and evidence of the objective condition of an event automatically (according to fixed events). It also captures information with embedded intelligent. The context of the environment is updated and the device will respond accordingly. Note that this is a continuous cyclic process.
- Connection and infrastructure: Cloud and its security, storage, privacy and processing make an interconnection together (for a real-time data and information flow and feedback) with connecting with the IoTs.
- Analytics and applications: The data generated by the sensor (enabled/embedded in Internet-connected devices) is gathered by the user. With the help of appropriate or efficient tools, it is transformed into information, which can be used for the purpose of analysis.

Further, the following enabling technologies with Internet-connected things/IoT are used, i.e. Radio-Frequency Identification (RFID), Wireless Sensor Networks (WSN), Addressing Schemes, Data Storage and Analytics, and Visualization. An Internet-connected/IoT device can be classified further into two categories:

- Physical objects: These can be smartphone, camera, sensor, vehicle, drone and so on.
- Virtual objects: These include electronic ticket, agenda, book, wallet and so on.

In the past decade, several security vulnerabilities are being found in Internet of Things/cyber-physical systems like robotics/electronic power grid, intelligent transportation systems, medical devices and so on [3]. Hence, remaining paper/work can be organized as follows: Sect. 2 discusses several applications of Internet of Things (in near future). Further, Sect. 3 discusses several security issues with Internet of Thing's devices (with suggested countermeasures). Further, Sect. 4 also discusses some serious issues like privacy, security (hardware, network, etc.) in IoTs ecosystem

in detail. Later, Sect. 5 discusses some challenges in IoTs and limitations of IoTs. In last, this work is concluded as Sect. 6.

2 Applications of the Internet of Things in Near Future

Some applications of the Internet of Things or Internet-connected things are everywhere in human being's life. Some of them are being discussed in this subsection. In [4, 5], the main IoT applications have been identified by several authors which are smart energy, smart health, smart buildings, smart transport, smart living and smart city (see Fig. 1). Successful realization of the vision of a pervasive IoT would require unification of these diverse vertical application domains into a single, unified, horizontal domain, often referred to as '*smart life*'. Based on inputs from experts, surveys and reports, the European Research Cluster (ERC) on the Internet of Things (IoTs) identified the Internet-Connected Things application domains. In [4], authors present an updated enumeration of the application domains. Hence, the uses of IoTs device can be discussed via several applications/domains:

- Cities *Smart Parking*: In this domain, IoTs can be used to monitor parking spaces availability in the city, monitor vibrations and material conditions in buildings,

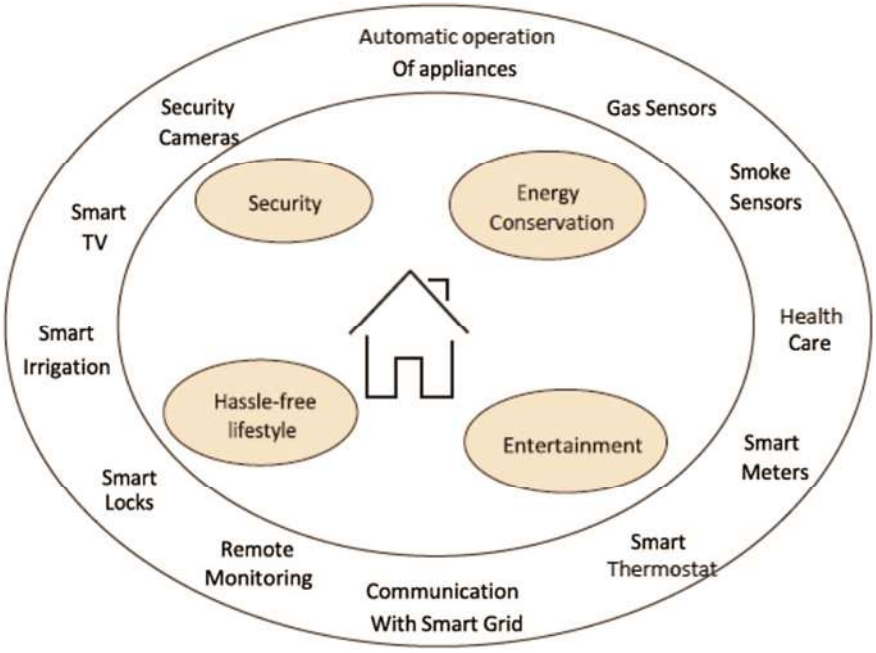

Fig. 1 Multiple application scenarios of Internet of Things

bridges and historical monuments (i.e. *Structural health*), to monitor real-time sounds in centric zones (or *Noise Urban Maps*), monitor vehicles and pedestrian levels to optimize driving and walking routes (i.e. to reduce *traffic over road network*), to make intelligent and weather adaptive street lighting (i.e. for *Smart Lightning*), to detect rubbish levels in containers to optimize the trash collection routes (or for *Waste Management*) and in *Intelligent Transportation Systems* (i.e. smart roads and intelligent highways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams).

- Environment and Water: In this domain, IoTs can be used to monitor flaming gases and pre-emptive fire conditions to define alert zones (to detect fire in *Forest*), to control carbon dioxide emissions of factories, pollution emitted by cars and toxic gases generated in farms (i.e. in reducing *Air Pollution*), to monitor soil moisture, vibrations and earth density to detect dangerous patterns in land conditions (i.e. *Landslide and Avalanche Prevention*), detect early e*arthquakes* via distributed control in specific places of tremors, study water suitability in rivers and the sea for fauna and eligibility for drinkable use (i.e. for improving *Water Quality*), detect presence of liquid outside of the tanks and pressure variations along pipes (i.e. to reduce *Water Leakages*), to monitoring water-level fluctuating in rivers, dams and reservoirs (*River Floods*).
- Energy Smart Grid, Smart Metering: In this domain, IoTs can be used in several applications like in monitoring water, in storing oil and gas levels in tanks and cisterns (i.e. with containing a *Tank level)*, to monitor and manage the energy consumption (i.e. for *Smart Grid applications)*, to monitor and optimize the performance of solar energy plants, to measuring water pressure with checking emptiness level (in pipelines systems, i.e. *Photovoltaic Installations)*, also to calculate weight of the goods (i.e. to measure *Silos Stock Calculation)*.
- Security and Emergencies: Internet-Connected Things/IoTs are also used for various other uses like to access the control on restricted areas and detection of people in non-authorized areas (i.e. as *Perimeter Access Control)*, for liquid detection in data centres or warehouses/sensitive building grounds for preventing any damages/break downs or corrosion. Also, it is used to measure the radiation levels in nuclear power stations via generating leakage alerts (i.e. with providing *Radiation Levels)*. In last on a large scale, it is also used for detecting gas levels/leakages in industrial environments (around chemical factories and inside mines) to find *Explosive and Hazardous Gases.*
- Retail and Logistics: Moreover, above uses, IoT devices are also used in some other applications like retail and logistics. It (IoT devices) is used to monitor storage conditions along the supply chain and product tracking for traceability purposes (i.e. in summary as *Supply Chain Control)*, for payment processing in applications like public transport, gyms, etc., (based on location/activity), also for receiving useful advice from the sale (like customer habits, preferences, presence of allergic components, etc.,), i.e. it may help in creating *Intelligent Shopping Applications/Smart Product Management. In last, IoTs are also used for* monitoring vibrations/strokes/container openings (or cold chain maintenance for

insurance purposes), also for searching of individual items in big areas like warehouses (with giving warning emission on containers which store inflammable goods/explosives).

- Industrial Control: IoTs used in some other domains like in machine auto-diagnosis and assets control, for monitoring toxic gas and oxygen levels (inside chemical plants to ensure workers' and goods' safety). Also, IoTs are used to control temperature inside industrial and medical fridges with sensitive merchandise with temperature monitoring, to monitoring the ozone levels during the drying meat process in food factories (ozone presence). Hence, in summary, IoTs are used to check indoor air quality, also in collecting information (from buses/transport devices) with sending real-time alarms (in case of emergencies), i.e. to provide suitable/best advice to drivers.
- Agriculture and Animal Farming: As the best usage of IoTs, it is implemented in agriculture and animal farming nowadays. With IoT devices, we can monitor soil moisture and trunk diameter in vineyards (i.e. to control sugar content in grapes and grapevine health), *to increase* production of fruits and vegetables and its quality (with decreasing impact of *Green Houses or with* controlling microclimate conditions. Also, IoTs can be used in studying weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes with controlling humidity and temperature levels in alfalfa, hay, straw, etc. (preventing soil from fungus and other microbial contaminants). In last, IoTs are also used in controlling growing conditions of the offspring (in animal farms), i.e. ensuring its survival and health*, also used in Animal Tracking (which are grazing in open areas).*
- Domotic and Home Automation: In this domain, IoTs can be used to monitor energy and water supply consumption to obtain advice on how to save cost and resources (i.e. to find total e*nergy and water use for a time span*), switch on and off remotely appliances to avoid accidents and save energy (i.e. in *Remote Control Appliances*), detect window and door openings and violations to prevent unknown users/intruders (i.e. *Intrusion Detection Systems*), to monitoring conditions inside museums and art warehouses (i.e. in *Preservation of Art and Goods*).
- *e-Healthcare:* In this domain, Internet-Connected Things can be used to assist elderly/disabled people living independently, control conditions inside freezers storing vaccines, medicines and organic elements (i.e. as *Medical Fridges*), monitor conditions of patients inside hospitals and in old people's home (i.e. having surveillance of *Patients*), measure ultraviolet (UV) sun rays to warn people not to be exposed in certain hours.

Hence, IoTs are used in several applications like: to control the routes followed for delicate goods like medical drugs, jewels or dangerous merchandises as *Fleet Tracking, in increasing agriculture cycle/*irrigation in dry zones with finding (requiring) actual water resources (with a measurement) or compared to green areas, to monitor vital signs in high-performance centres and fields, *to s*tudy air quality in surrounding areas/farms and detection of harmful gases from excrements, i.e. to know level of *Toxic Gases,* etc. This section discusses several applications of Internet of Things

with respect to real-world problems. Now, next section will discuss several issues raised in IoTs (with suggested countermeasures/solutions) devices in detail.

3 Popular Security Issues with Internet of Thing's Devices (with Suggested Countermeasures)

Taking many devices under a user's control (via several security attacks like DoS, eavesdropping, DDoS, etc.) for his financial gain raised issues of security. Also, tracking user's every step (i.e. an issue of privacy) is the biggest issue among available issues in IoT devices. In general, IoT devices have made human life better and better (in terms of living standards). But, when these devices integrate with several other IoT devices and used by many users (in parallel mode), then they create (collect/capture) a lot of data which may leak to malicious/unknown/ and can be stolen by any hacker. This is also a critical issue to overcome. Hence, in IoT, issues like not having proper standards for hardware used with IoT to make a communication, poor system security, server security, data security, leaking of user's personal information, etc., need to be overcome (attention from research community) in near future.

3.1 Insecure Web Interface

Internet of Things or Internet-Connected Things/devices having a web interface which allows a user to interact with the device (person to device communication). But at the same time, it (smart devices) could also allow an attacker/malicious user to gain unauthorized access to the connected smart devices. Some of the issues which may arise due to security vulnerabilities are Account Enumeration, Weak Default Credentials, Credentials Exposed in Network Traffic, Cross-site Scripting (XSS), SQL-Injection, Session Management and Weak Account Lockout Settings [6]. As solution, these security vulnerabilities can be avoided by using countermeasures like the default passwords and usernames should be changed during the initial setup only (with ensuing a reliable, secured password recovery mechanism). Here, no weak passwords are allowed, especially a combination of letter, number and special character needs to be considered for a strong password mechanism. The account should be lockout after 3–5 login attempts and to ensure that web interface is not susceptible to XSS, SQLi or CSRF.

3.2 Unsatisfactory Authentication/Authorization

Some ineffective or insufficient mechanisms exist to authenticate the IoT user interface. It is a part of poor authorization mechanisms, i.e. where a user can gain higher levels of access, where he is allowed only for few. Some security vulnerabilities can create this issue which are Lack of Password Complexity, Poorly Protected Credentials, Lack of Two-Factor Authentication, Insecure Password Recovery, Privilege Escalation and Lack of Role Based Access Control [6]. Hence, these security vulnerabilities can be avoided by using countermeasures like first assure that the password is strong (enough), and then ensure access control wherever and when it (password) is necessary. Further, assure that the credentials are properly protected with a strong encryption mechanism. We can apply two-factor authentications wherever possible to provide higher security. Later, we can ensure that the mechanism for password recovery is also secure. Note that we need to ensure also re-authentication for some sensitive features, i.e. options for configuring password controls (if the user forgets the password).

3.3 Insecure Network Services

In this, a user wants to access the IoT device, then the device might allow him/an intruder to gain unauthorized access to the device or its associated data. Some security vulnerabilities that can create this issue are Vulnerable Services, Buffer Overflow, Open Ports via UPnP (Universal Plug and Play), Exploitable UDP (User Datagram Protocol) Services and Denial of Service/DoS via Network Device Fuzzing. Hence, these security vulnerabilities can be avoided by countermeasures like ensure that only necessary ports are available, and given services to devices are not malicious to perform any DoS attack, overflow and fuzzing attacks. Also, we need to ensure that available network ports/services are not exposed to the Internet (via UPnP) or to a third party (to unknown user).

3.4 Lack of Transport Encryption

Exchanged data with the IoT device can be available or transfer to other devices in an unencrypted format. This could easily lead to an attacker/intruder sniffing the data and either capturing this data for later use or compromising the device itself. Some security vulnerabilities that can create this issue are Unencrypted Services via the Internet, Unencrypted Services via the Local Network, Poorly Implemented SSL/TLS and Misconfigured SSL/TLS. Hence, these security vulnerabilities can be avoided by solution like ensuring data/information is encrypted using efficient protocols (Secure Sockets Layer (SSL), Transport Layer Security (TLS)) or any

another standard encryption algorithms/security protocols (if SSL and TLS are not available) while transiting in network to other network or from a device to another device. Hence, we need to ensure that only accepted or standard encryption standards have been used (to avoid any kind of attacks) in IoT devices.

3.5 Privacy Issues

Privacy issues are raised in generated of personal data [7, 8] by millions of IoT devices. Today, we are lacking in protection of this data (properly and with higher security). Privacy issues can be found in IoTs by analysing the data (collected when a user makes set up and use the respective smart device for communication). Several automated tools or feature of smart devices are being used to look or track specific patterns of user. This continuous tracking of a user produces a lot of data that may contain some sensitive information of user. Some security vulnerabilities that can create this privacy issue are collection of irrelevant personal information, sharing personal information of user with malicious devices/users, etc. Hence, these privacy issues/vulnerabilities (in a network) can be avoided by using mechanism like ensuring that data collected by devices is general, and is not sensitive/personal data (also should be de-identified or anonymized). Also, ensure that (always) data is collected through proper mechanism/encryption schemes and only authorized/known users need to access/permitted to use this data/personal information. In last, we need to ensure that end users are provided with 'Notice and Choice' if data collection is more (in storage) than what would be expected from the devices/products. Note that always we need to ensure that smart devices (or IoTs) and its components are storing, retrieving and protecting its data properly.

3.6 Insecure Cloud Interface

Today, several security issues are raising related to the cloud interface (which is in interaction with IoT devices). It may provide poor authentication controls/data travelling in an unencrypted format, i.e. allowing an attacker access to the device or the underlying data. Some security vulnerabilities that can create this issue are Account Enumeration, No Account Lockout and Credentials Exposed in Network Traffic [6]. Hence, these vulnerabilities/attacks can be avoided by using solution like the default passwords and usernames need to be changed during initial setup (as mandatory). Then, we need to ensure that there should be enough and efficient functionality, i.e. password reset mechanisms in user accounts and locking of account (in case of after 3–5 failed login attempts). Also, we can implement two-factor authentications, if possible/required. In last, we can ensure that cloud-based web

interface is not susceptible to ay attacks like XSS (Cross-Site Scripting), SQLi (SQL-Injection) or CSRF (Cross-Site Request Forgery) (including that no credentials are exposed over the Internet/World Wide Web).

3.7 Insecure Mobile Interface

Weak authentication or unencrypted data channels can allow an attacker access to the device or underlying data of an IoT device that uses a vulnerable mobile interface for user interaction. Some security vulnerabilities that can create this issue are Account Enumeration, No Account Lockout and Credentials Exposed in Network Traffic. Hence, these vulnerabilities can be avoided by following countermeasures:

a. Assure credentials should not be exposed while connected to wireless networks.
b. Countermeasures from (a)–(d) of Sect. 3.6.

3.8 Insufficient Security Configurability

Insufficient security configurability is present when users of the device have limited or no ability to alter its security controls. Insufficient security configurability is present when the web interface of the device has no options for creating granular user permissions, for example, forcing the use of strong passwords. The risk here is that IoT device could be easier to attack allowing unauthorized access to the device or the data. Some security vulnerabilities that can create this issue are Lack of Granular Permission Model [6], Lack of Password Security Options, No Security Monitoring and No Security Logging. Hence, these vulnerabilities or attacks can be avoided by using suggestions like we need to ensure that ability to separate normal users from administrative users or another (malicious) user. Then, we need to ensure that the ability to encrypt data at rest (server side) with containing strong password policies to increase security (i.e. ability to send security alerts of logging events to end users).

3.9 Insecure Software/Firmware

The lack of ability for a device to be updated presents a security weakness on its own. Devices should have the ability to be updated when vulnerabilities are discovered and software/firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/firmware can also be insecure if they contain hardcoded sensitive data such as credentials. The inability of software/firmware being updated means that the devices remain vulnerable indefinitely to the security issue that the update is meant to address. Further, if the

devices have encoded sensitive credentials, if these credentials get exposed, then they remain so for an indefinite period of time. Some security vulnerabilities that can create this issue are Encryption Not Used to Fetch Updates, Update File not Encrypted, Update Not Verified before Upload, Firmware Contains Sensitive Information and No Obvious Update Functionality. These vulnerabilities can be avoided by using solution like we need to ensure that device has the ability to update automatically or with user permission (mandatory). Further, we need to ensure that update file is encrypted using accepted/standard encryption method (or update file is transmitted via a reliable encrypted connection). Note that we need to ensure that update file does not contain or expose any sensitive data to any user/device, also verified that any updation in device is signed and verified (with a secure update server).

3.10 Other Security Issues in Internet of Things

Providing security in IoT devices is a critical and an essential issue to solve for winning trust among people and organizations. The application data of IoT could be industrial, enterprise, consumer or personal. This application data should be secured, with reliable privacy preserved schemes (as confidential against any kind of attacks like theft or tampering). As discussed in [4, 2], IoT devices/applications may store the information of end users, for example, the information/results of a patient's health or shopping store. Today's smart devices like IoT have improved the communication between devices. But with this they (IoT devices) have created several issues like scalability, availability and response time. Security is a concern where the data is securely transmitted over the Internet. Issues like privacy (leaking of personal data of users) and data sharing with others raise the issue of trust in IoT ecosystem.

Hence, this section discusses popular security and other issues with suggested solutions in Internet of Things. Now, next section will discuss some top (popular) issues with respect to security and privacy in an IoT ecosystem.

4 Security and Privacy Issues in Internet of Things Ecosystem

As discussed in [4] and several IoTs applications (refer Sect. 2), Internet-Connected Devices/Things can communicate together/with consumers, and may share data back to respective service providers (or master: who build these devices), and compile data for third parties such as researchers, healthcare providers, firms, organizations or even other consumers. For example, in past, there were several rumours that Xiaomi (a mobile company of China) is storing and passing user's personal data/information to China's government. Hence, the storing and sharing of information with smart devices/IoT devices bring new challenges for regulators, enterprises and consumers.

As we know (discussed), the IoT revolution is already under construction, i.e. not implemented completely. *'Things' (e.g. everyday objects, environments, vehicles and clothing) will have more and more information associated with them, and are beginning to sense, communicate and produce new information, to become an integral part of the Internet.* In near future, market of IoT devices will reach £200 billion annually (worldwide), with introducing new business models, being implemented in several applications and providing efficient services to each area/sector of the economy (of a country). These will also stimulate innovation and growth in areas such as components, devices, wireless connectivity, system integration and decision support tools. Some serious issues with IoTs need to overlook by research communities (for providing smart, secure communication) are included as follows:

a. Device/Physical Security: Connection devices are main components of IoT, which collect data and interact with other devices/humans. When these devices collect data, then they are so vulnerable to physical security issues. Note that when we have a robust network, at that time also unauthorized physical access to connected IoT devices can be happened/traced. This may create problem of catastrophic system failure. Hence, some ways to ensure physical security are limiting physical access to the device, and ensuring proper security measures in the Operating System (OS) to prevent unauthorized access. Generally, physical security weaknesses are available when a malicious user/attacker can disassemble a device to easily access the storage medium and any data stored on that medium. Weaknesses are also present '*when Universal Serial Bus (USB) ports or other external ports can be used to access the device using features intended for configuration or maintenance. This could lead to easy unauthorised access to the device or the data'. Some security vulnerabilities that can create this issue are Access to Software* via *USB Ports and Removal of Storage Media*. Hence, these vulnerabilities can be avoided by following countermeasures:

   i. Ensuring medium of data storage (it should change frequently) and this (collected/stored) data need to properly encrypt (at server side), i.e. using secure cryptographic mechanism.
   ii. Ensuring USB ports/other external ports cannot be used to maliciously access the device.
   iii. Ensuring device cannot be easily disassembled and provide limit use of data to administrations/authorized users.

b. Network Security: Networks are always vulnerable to hacks from long decades (i.e. before advent of IoT). Several hackers tried to occupy network for their financial use. We have large volume of IoT devices, which makes us have a robust and secure network. In the past decades, several scientists and researchers had analysed about security components (to various components). They found that vulnerability in network is due to weakest link/in processes/transferring of a data (in source to final destination). A network can be exploited by malicious users/hackers via remotely, i.e. without access of IoT device physically [9]. One better solution for proper security/avoiding network compromise is to use Virtual

Private Networks (VPN's). It secures a network by encrypting the data traffic that flows through them [10]. Note that VPNs do not ensure absolute security to a system/network, i.e. still susceptible to Man-In-The-Middle (MITM) attacks.

c. Data Security: Data in IoT can be classified into two categories: stored data (data at rest) and data in the process of transmission (data in flight). For maintaining data integrity, we need high-level encryption of both data types. But, problem of scale raised here, i.e. with a large variety of devices and varying hardware specifications, it is clearly impossible to create a one-size-fits-all standard data encryption process. Data which is highly sensitive like bank account details, usernames and passwords are required to encrypt with two (or more) factor authentication processes to ensure security.
d. Operating System Security: Operating Systems (OS) are prime target for any malicious user/attacker/hackers. If a hacker gaining access to the OS of an IoT cluster/a single device, then attacker can exploit or compromise into a system/own a system (can run according to his/her commands). Note that recovering from OS security breaches is so costly (it may lead to partial/complete data loss), and also require a lot of time to restore an OS to full efficiency. Here, backups of a system can minimize the overall cost of recovering from an OS hack. Whereas it is impossible to accurately detect the date of a hack/compromise, and also it is impossible to know the exact point from which (or where) a system can be restored. Hence, with the increasing size and complexity of IoT devices, a more robust IoT security analytics process is required to identify and neutralize IoT specific security breaches in near future.
e. Server Security: Nowadays, IoTs are working as smart devices and interacting with cloud servers. Here, Denial-of-Service (DoS) attack is one of the dangerous attacks that affect servers, i.e. malicious users use a large number of proxy devices to generate fake requests to the server. It makes server as ineffective, i.e. server is unable to attend requests of real users or got hanging problem due to the high overhead. Several steps have been taken to protect server security which include limiting the number of open ports and exposed services. Here, security configurability needs to be a primary issue to solve, i.e. when an IoT system is being developed with allowing systems to be updated remotely with proper encryption and validation of update files.

Hence, a large amount of data (called big data: in 2005 Roger Mougalas from O'Reilly coined this term first time [11, 12]) produced by IoT devices (from everyone), which is a challenge for all software testing Services Provider (SP) to provide enough security to all system/IoT devices. With IoT security analytics, remote monitoring systems and automated patching procedures, we can secure IoT systems. However, security challenges in IoT (developing) systems will be grown in near future (because use of IoT and building of IoT are in initial stage only). It will increase complexity in solving any issue/to create new/updating existing security countermeasures to protect IoT technologies. Note that IoT security issues can be available with different natures and occur at different levels. So, every organization/firm/company in the IoT sector

must ensure the security, privacy and experience of users so that we can really take advantage of the benefits of the Internet of Things.

Hence, this section discusses several popular issues raised with Internet of Things. Also, this section tries to provide (maximum) countermeasures and possible solutions to each/respective issues. Now, next section will discuss several challenges noticed/rectified in IoTs (or Internet-Connected Things).

5 Challenges in Internet of Things

Internet of Things is a very complicated heterogeneous network platform. It is connected and being used in several beneficial applications like smart home, smart metering, smart farming, smart transportation, etc. Some other cloud computing challenges are architecture, energy efficiency, security, protocols, quality of service and standardization of frequency bands and protocols. Moreover this, various security challenges have been discussed by Misra et al. in [13]. Note that as an interconnection of highly heterogeneous networked entities (IoT devices), it follows a number of communication patterns: Human-To-Human (H2H), Human-To-Thing (H2T), Thing-To-Thing (T2T) or Thing-To-Things (T2Ts) [4]. Providing efficient services among such integration (of devices and human being) is a challenging task. In last, battery life extension and lightweight computation are the major limitations of IoT devices, so to make efficient IoT devices with less consumption of energy is also a challenging task. In last, several types of attacks like passive, man in middle, eavesdropping, active, gathering, etc. with possible solutions have been discussed in [7]. Now, next section will conclude this work in brief.

6 Conclusion

Today, we are living in an era of smart world, where all devices are connected together through Internet. These devices are helping human being and making their life easier. In summary, we can say that these Internet-Connected Things (ICT) devices or Internet of Things (IoTs) devices (in integration or connecting together) have made human life easier, better and safer with introducing several applications like smart homes, smart parking, smart transportation, smart cities, smart farming, smart grid, etc. But, using such (smart or Internet connected) devices in our daily life, people are very much concerned about ‘their personal or sensitive information’. So a question raised here: ‘Is it (personal information) safe with these devices?’ When things (i.e. these Internet-connected smart devices) react to environment, data will be captured and transformed into valuable insights, which can be shared/utilized in various applications/domains, i.e. ranging from automated home appliances, smart grids (including high-resolution assets), in increasing production of a firm, to increase growth of economy of a nation with product management, etc. Also, manufacturers

of such devices can collect data generated from these devices for their future use, for example, washing machine's manufacturers/companies collect status of machine to improve their future product (for targeting new customers in future). Hence, in this paper, we have discussed some challenges, security and privacy issues which are needed to be overcome and require attention form research community. In near future, we can focus such issues to do our future research work (i.e. to enhancing the present stance of IoT by incorporating security and privacy into its current design and implementation).

References

1. TELEFÓNICA I+D: Internet of Things + Internet of Services (2008).
2. Tyagi, A. K., & Shamila, M. (2019). Spy in the crowd: How user's privacy is getting affected with the integration of internet of thing's devices. In *SUSCOM-2019: International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM-2019)*. Amity University: Rajasthan, India (26–28 February 2019).
3. Vermesan, O., Friess, P., Guillemin, P., et al. (2011). Internet of things strategic research road map. *Internet of Things: Global Technological and Societal Trends, 1,* 9–52.
4. Tyagi, A. K., Anuradha, N., Rekha, G., Sharma, S., & Sreenath N. (2019). How a user will look at the connection of internet of things devices?: A smarter look of smarter environment. In *ICACSE: 2019 2nd International Conference on Advanced Computing and Software Engineering, KNIT Sultanpur, 2019*, India (8–9 February 2019).
5. Kocovic, P., Behringer, R., Ramachandran, M., & Mihajlovic, R. (2017). *Emerging trends and applications of the internet of things*. IGI Global Book.
6. https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/.
7. Tyagi, A. K., Rekha, G., & Sreenath, N. (2019). Beyond the hype—internet of things concepts, security and privacy concerns. In *Proceeding of Springer/International Conference on Emerging Trends in Engineering, College of Engineering (ICETE)*, Hyderabad, Telangana, India: Osmania University (22–23 March 2019).
8. Moura, J., & Serrão, C. (2016). Security and privacy issues of big data.
9. Veerendra, G. G. *Hacking internet of things (IoT), a case study on DTH vulnerabilities*, SecPod Technologies.
10. https://www.senetas.com/network-traffic-flow-analysis-protection-enhancesencryption/.
11. https://datafloq.com/read/big-data-history/239.
12. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management, 35*(2), 137–144.
13. Misra, S., et al. (2017). Security challenges and approaches in internet of things. *Springer Briefs in Electrical and Computer Engineering*. https://doi.org/10.1007/978-3-319-44230-3_2.

Study of Information Retrieval and Machine Learning-Based Software Bug Localization Models

Tamanna and Om Prakash Sangwan

Abstract Software bug localization (SBL) is a process of finding out the location of bug that causes the failure of some functionality in the application. There are many different methods of performing SBL like analysing of execution traces, information retrieval and manual debugging. Information retrieval (IR) based models works as same as simple search query model in which bug report is taken as query. In this paper, we perform an empirical study for verifying the effectiveness of VSM. Based on TFIDF modelling, the results are experimented on four datasets and evaluated with TOPK, MAP and MRR metrics. In addition to this, review of existing machine learning and deep learning-based SBL models are also presented because of their effective power and improved results in localization accuracy.

Keywords Vector space model · GLOVE · Word embedding · Software bug localization (SBL) etc.

1 Introduction

SBL is one of the crucial tasks for software developers searching for a particular instance, which cause failure is called debugging or software bug localization. Exponential increase in open-source software projects and code result in the need of software developers in this field also. Traditional debugging methods were manual and time consuming. Therefore, automate debugging come into the existence for making the localization process faster and leads in better utilization of resources. Different state-of-the-art localization models are proposed but till date, no one is robust or have one for all model is built. Active research is going on in this domain of IR-based SBL in association with soft computing techniques like machine learning,

Tamanna (✉) · O. P. Sangwan
Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, Haryana, India
e-mail: tamannasharma100@gmail.com

O. P. Sangwan
e-mail: sangwan0863@gmail.com

H. Sharma et al. (eds.), *Advances in Computing and Intelligent Systems*,
Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-15-0222-4_47