An Analysis of Providing Security for Cloud-Based IoT Applications: A Prototypical Approach

Raviteja Gaddam[1], M. Nandhini[2]

[1,2]*Department of Computer Science, Pondicherry University*

(E-mail: raviteja.csebec@gmail.com)

***Abstract*—**Innovations in technology made possible to connect everything. Internet of Things (IoT) is promising to connect and communicate any device from anywhere using the Internet. IoT can be a new era of the world and it influencing our lifestyles. Billions of devices are connecting and the count is still increasing. This tremendous connectivity can not only make our lives better but also raising several security problems. Most of the IoT devices use the Cloud to store and analyze the data. And to communicate among them and to synchronize, Cloud is one of the best possible options. During data en routing, there are several possibilities for data breaches. It is critical to ensure end-to-end security for IoT applications. In this paper, authors discuss the possible challenges in providing security and privacy for Cloud-Based IoT applications and propose a model to reduce the risks.

Keywords*—Internet of Things; Cloud; Security; IoT Applications*

I. INTRODUCTION

IoT drives the embedded computing devices of our daily life objects to communicate and transfer the data. Technological advancements in Sensors, Communication Protocols, and Networks make the IoT bridge the diversified technologies and empowering novel applications to support intelligent connectivity among physical objects. According to CISCO IBSG Projections, exponential growth in interconnected devices make them nearly 50 billion [1]. This massive communication tremendously creates vast opportunities for economic growth. McKinsey Global Institute estimated that IoT can raise the revenue from 3.9 trillion dollars to 11.1 trillion dollars by 2025 [2]. Various State and Central Governments harness the benefits of IoT with social and economic development.

This greater connectivity also raising several security challenges to IoT devices. According to CISCO Cybersecurity Report 2018, IoT botnets are expanding along with the IoT and becoming more mature and automated [3]. As they grow, attackers are using them to launch more advanced attacks. We can imagine how big the impact is if data breaches and security incidents occur in billions of devices connected network. IoT devices have a very serious threat. According to SOPHOSLABS 2019 Threat Report, VPNFilter Malware affected a broad class of home and small business networking devices in 2018 brought the home the potential impact of malware that could persist on [4]. As the number of interconnecting devices increases, there is more necessity for IoT Security.

As the IoT devices have limited resources like storage, computation power, and memory, they are utilizing the Cloud for storing the data and synchronize among them. To ensure privacy and data security for IoT applications, it is important to secure IoT devices. As the data generated by IoT devices transmitted to a cloud-based storage facility, there are several possibilities for data breaches while enrooting to cloud. So, it is essential to ensure the security and end-to-end trust for IoT applications. To ensure them, authors discuss various security challenges and propose a model to and discuss several ways to minimize the risks.

This paper is organized as follows. Section 2 discusses some recent works in Cloud-based IoT applications. In Section 3, we discuss an architecture related to IoT applications followed by a proposed model in Section 4. In Section 5, we discuss various challenges and issues in providing security for IoT applications followed by a conclusion in Section 6.

II. RELATED WORK

In this section, we discuss various recent works on cloud-based IoT applications and try to analyze several issues regarding security in IoT based networks.

Authors of [5] proposed FPGA Scheme to secure public cloud-based IoT applications against several attacks. Authors discussed using different keys for symmetric re-encryption while transmitting the data from IoT devices to Cloud storage. Various countermeasures were discussed to prevent the attacks like Cryptographic Attacks, Replay Attacks, Tampering, Cloning, and counterfeiting. Experimental results have shown promising performance but the scheme may not be reliable in high bandwidth network where the en route of data to the cloud is faster than sharing the keys and encryption.

L. Peng et. al in [6] discussed the possibilities of integrating Fog and Cloud Computing to provide efficient data storage for IoT applications. Authors presented a new architecture called iCloudFog that integrates Fog and Cloud. This architecture was mainly composed of the access network and IoT devices. But they haven't discussed several challenges like security, network dimension, localization and resource management.

In [7], authors have presented a flexible middleware framework for securing IoT applications. This middleware connects the backend Fog communication with IoT devices. Authors used a Session Resumption algorithm that can reuse the sessions while transmitting the data from IoT devices to Fog. Experiment results have shown the resumption of encryption schemes in a resource-aware environment. But in real time environment where the devices are more and the network is huge, this scheme may work slowly because of maintaining session information for all the devices.

L. Bittencourt et. al in [8] have discussed the possibilities and challenges in integrating IoT devices, Fog and Cloud. They presented the analysis of how the combination can reduce the bottlenecks in communication and data transfer. Authors emphasized the three facets of integration: Infrastructure, Management, and Applications. Infrastructure-focused on IoT devices, Cloud, Fog nodes and communication protocols. Management focused on Resource Allocation, Serverless Computing, Energy Consumption, Data Management and applying regulations and trust models. Applications discussed Urban Computing, Mobile Applications and Industry related IoT.

Hanan Elazhary discussed various directions towards integrating IoT devices, Cloud, Fog, Mobile IoT and Mobile Edge to ensure better performance in IoT applications in [9]. According to the author, all these areas are intersecting and emerging as powerful computing paradigms. He also emphasized various IoT technologies like Ubiquitous Computing, Pervasive Computing, Wireless Sensor Networks, Internet of Nano Things, and Internet of Underwater Things. The author made an extensive analysis of more than 400 research works and put various issues in integrating all the stated domains for better performance.

Authors of [10] have described various Collaborative IoT applications that were related to various domains like Smart Cities, Smart Energy, Health and Fitness, Smart Infrastructure, etc. they mentioned some Software Stacks for monitoring fitness and health like automated wearable devices. Health monitoring can be done both at the individual level and business level like hospitals. Home Automation with Smart Thermostat, Smart Smoke Alarm, and Smart IP Camera. For building automation, we can use Smart Energy to reduce drown outs. Challenges like security and autonomy will question the reliability of IoT devices. At the business level using service boats can improve the manufacturing process. Authors suggested using various solutions like IPSec, Firewall, Secure Booting, and Anti-Tampering Devices to provide better security in the IoT network.

In [11], the authors proposed a Role Based Encryption to secure the Cloud-Based Storage for IoT applications. Main components considered by the user for this work were IoT devices, Network Infrastructure, Gateways, and Cloud Storage. While designing this system, a role manager will be created whose responsibility is to assign roles to the authenticated users while accessing the data. Authors used AES and RSA algorithms for encryption of data during uploading to the Cloud. The drawback of this approach is the high computation requirement of the combined use of this algorithm in the resource-constrained IoT devices.

Authors of [12] discussed the usage of Cloud hosted Hadoop system to land and cleanse the data generated by the enormous IoT devices. This may incur with extra work of storing the data in HDFS to enable the usage of Hadoop services. Policies were separated to ease the management of Security and Data analysis.

Jun Zhou et. al discussed various challenges and countermeasures in providing security for Cloud-Based IoT applications in [13]. Authors proposed architecture for secure packet forwarding without using public key encryption. To handle various threats, authors suggested solutions like Pseudonym, game theory and privacy-preserving authentication. Major challenges identified were designing lightweight encryption, location privacy, data confidentiality and supporting next-generation communication technologies.

Chiara Bodei et.al discussed a methodology to measure the possible risks of IoT and their countermeasures in [14]. Authors discussed IoT-LySa language based on algebra to design and specify a network of smart objects. By considering quantitative factors and tried to infer the possibilities of different implementations of IoT Systems. Authors applied the methodology to a Smart Store example and assessed the performance and energy consumption.

Authors of [15] tried to improvise the offloading efficiency during the data transmission in Cloud-based IoT applications. This paper mainly focused on developing a data transmission scheme STOFDM, Secure Truncating Orthogonal Frequency Divisional Multiplexing to truncate the OFDM signal. Simulation results of this Fast Fourier Transformation based STOFDM have shown low complex computation but as a whole computing offload of IoT based Cloud has to be reduced.

Christos Stergiou et.al discussed various issues in integrating Cloud-based Storage for IoT applications in [16]. Authors surveyed several research works and identified the problems related to security and privacy in using Cloud storage as a backend for IoT applications. They tried to map the common features of IoT and Cloud for better integration. Identified various challenges such as performance, reliability, heterogeneity, and huge data and monitoring. They proposed a model to encrypt the transmitting data using AES and RSA but this approach may not be suitable for the resource-constrained IoT devices.

III. IOT APPLICATIONS ARCHITECTURE

A basic and general architecture of IoT applications is shown in Figure 1. Here we discuss this architecture in different perspectives like domains, communication models and security.

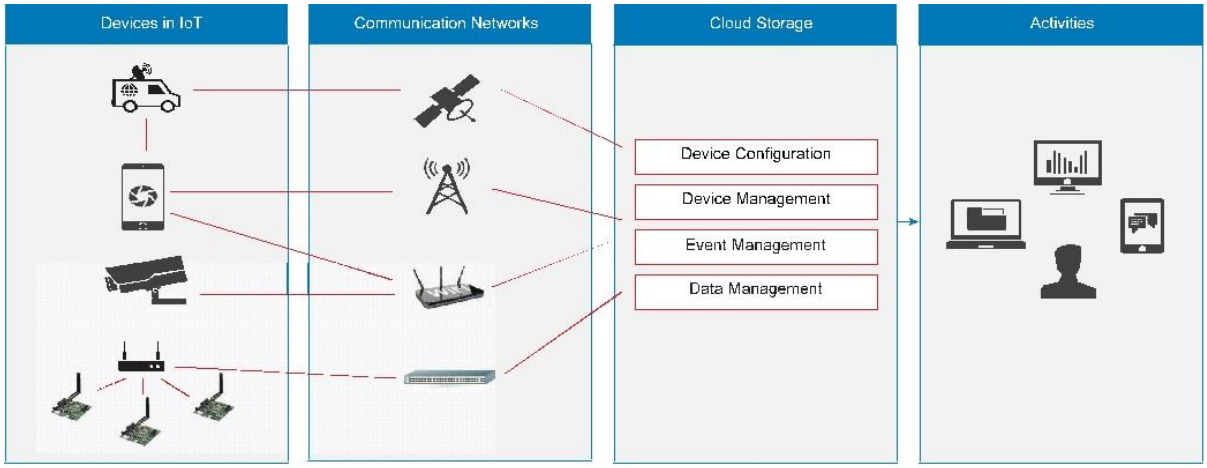

Figure 1. IoT Applications Architecture

A. Domains:

From Figure 1, we can observe that mainly four domains comprise the architecture and they are Devices in IoT, Communication Networks, Cloud Storage and Activities.

1) Devices in IoT

This domain involves various devices that are involved in various applications like sensors to medical devices. These devices differ in sizes, OS, and protocols. These devices are arranged to work in open environments. This diversity in IoT devices leads to several problems like interoperability, security, and reliability.

2) Communication Networks

IoT devices connect through this domain. As the communication to be done among the IoT devices and to Cloud Storage is a great challenge for the networks. Wi-Fi, Bluetooth, Cellular Networks are the major technologies for IoT devices communication.

3) Cloud Storage

As the limited resources constrain the functionality of IoT devices, the Cloud gives enormous storage and processing power. Thus the Cloud Storage domain provides facilitates like Device Configuration, Device Management, Event Management, and Data Management. IoT and the Cloud can be treated as two sides of the same coin. Cloud Service Providers integrate IoT devices to the Cloud by providing APIs. Google Cloud IoT is an example of IoT specific Cloud platform [17].

4) Activities

By running Cloud-based applications, data can be accessed by the end users on their laptops or desktops. Also, they can manage IoT devices by performing functions like activating or deactivating the IoT devices.

B. Communication Models:

According to the Internet Architecture Board (IAB), there are four types of communication models for IoT devices. They are device to device, device to the gateway, device to cloud and backend data sharing.

1) Device to Device Model

Here the communication between two devices is direct without any intermediary. Protocols like Bluetooth, Zigbee are often used for wireless communication. This type of model is most suitable for Smart Home Systems, Smart Watches, Smart Electrification, etc. where the data size is small and throughput is low.

2) Device to Gateway Model

Here Cloud Services are accessed by the IoT devices using gateways. The main purpose of these gateways is to aggregate the collected data, storing data in the cloud, communicating devices with different protocols, and providing security. In some situations, gateways communicate among them while relaying the data.

3) Device to Cloud Model

Here the data generated by IoT devices can be filtered by users with some rules and can take necessary actions through a Cloud Portal. There is a possibility of the occurrence of network congestion due to the continuous data generation by these devices. So the traffic must be monitored at regular intervals and necessary actions have to be taken to reduce the traffic jams.

4) Backend Data Sharing Model

The data generated by IoT devices may be isolated from other applications due to uploading data to a specific cloud service. This model can be considered as an extension to the earlier model. It allows sharing of generated data among trusted parties and users to analyze the data from various applications.

C. Security:

IoT applications where Cloud-based Storage is used, the data generated by IoT devices is transferred to the Cloud facility over the communication network. During this en route, there may be possibilities for data breaches. Hence, providing security for IoT applications in an end to end manner is essential. But, there are several threats to each domain. Vulnerabilities in Hardware and Software, DoS attack are few

of them in IoT devices domain and communication domain. The main reason for data breaches in the cloud domain is not complying with the regulations. Stealing users' credentials by the attackers and overtaking the IoT devices are few in Activities domain.

IV. IOT THREAT MODEL

To focus on improving the security measures for Cloud-based IoT applications, we propose a Threat Model as shown in Figure 2, which emphasizes three main domains: Security Features, Levels of Attacks and Attack Sites.

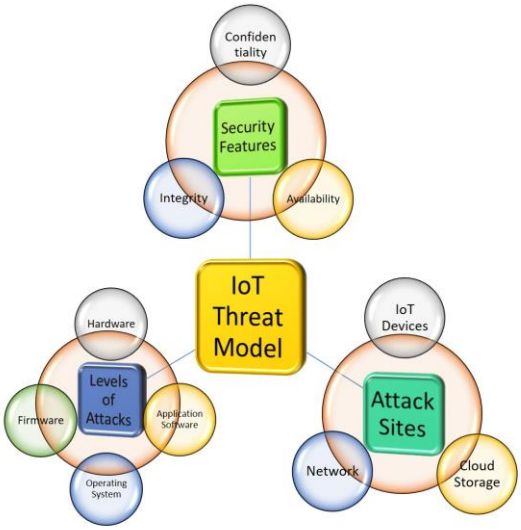

Figure 2. IoT Threat Model

A. Security Features

Providing Information Security means guaranteeing Confidentiality, Integrity, and Availability. Confidentiality ensures only authorized persons can access the data. Integrity ensures the data is accurate and it is not altered during transmission. Availability ensures the services and data are available for the end users who need it. If attackers compromise these three features then they can manipulate everything for their benefits. Impact of this can result in loss of end users' trust and business operations.

B. Levels of Attacks

The levels of attacks include four aspects: Hardware, Firmware, Operating System and Application Software. To make IoT Applications secure, these phases must be secured. Developers must test the security of IoT devices during the design and production phase.

1) Hardware

IoT security may not be ensured only with software-based approaches. An attacker can tamper device hardware if it is physically accessible and can change the settings so that it becomes unreliable. To avoid this risk, developing tamper-proof hardware is very much essential.

2) Firmware

Beyond tampering the physically accessible devices, sometimes attackers can get the content of internal memory and firmware by running clever programs through the onboard interface. This process gives them more knowledge about the device functionality. By using this, they can manipulate the firmware to get full control over it. For more effective attacks, they can access device security keys and backdoor of firmware. Attackers can also modify configuration settings and they might be able to customize the device settings to en route the data to their own storage facility.

3) Operating System (OS)

Most of the Internet-connected devices have their customized Operating System. Along with the proprietary OS like Windows, there are Open Source OS like Android, have their IoT versions [18] [19]. To meet the constraints of IoT devices like small memory, vendors are developing scaled down versions of these OS and neglecting the inculcating of security features. This eventually making the IoT OSs more vulnerable to threats.

4) Application Software

Most of the IoT devices are accessible to the end users through their respective applications designed and developed by the vendors. For example, a Smart Home app that can monitor the home electronics like AC, Lights, etc. gives an interface to the end users to interact with them. If the designing of this application is poor, then it can let unauthorized people control the devices. The consequence of these vulnerabilities makes the application hard to defend the attacks.

C. Attack Sites

As shown in Fig 1, IoT Application Architecture mainly includes the essential components: data generating IoT devices, data transferring Communication Networks, storing and analyzing Cloud Services and application-oriented activities. These applications can be accessed from any computing devices through the Internet. To provide security, this domain focus on the possible attack sites like IoT Devices, Network, and Cloud Storage.

1) IoT Devices

There is a huge rise in the attacks happening on IoT devices. Most of the IoT devices are communicating through the Internet for sharing the data. Security vulnerabilities in these IoT devices are making them as the primary target for many cyber criminals. Also, the possible physical accessing the devices is making them easy to tamper and hard to defend the attacks.

2) Networks

During data transmission from IoT devices, attacks like modification, DoS, injection, replay attacks, etc. are making the IoT applications unreliable. This tampered and falsified data is questioning the integrity of the collected and analyzed data. This can jeopardize the trust of end users.

3) Cloud Storage

To store and analyze the huge volume of data generated by IoT devices, Cloud is one of the best possible options. If the attackers compromise the data in the Cloud, then the consequences may threaten the existence of the organization. All the Cloud services are provided to the end users through web-based applications. During accessing these services, if cybercriminals compromise the user credentials, inject malicious code or break the authentication, the Cloud providers may become the victims of possible attacks.

The main goal of this model is to give a perspective of the possibility of attacks. For a broader perspective of providing security for Cloud-based IoT applications, we can also extend the analysis by including various network devices and Cloud platforms like SaaS, IaaS and PaaS.

V. IOT SECURITY CHALLENGES

To prevent data breaches related to IoT devices, many governments have initiated several steps. Even though providing complete security is remaining difficult, in this section, we try to discuss possible IoT security challenges.

A. Resource Constraints:

Providing security features Confidentiality, Integrity and Availability is not that simple by using cryptographic techniques. Because of the limited memory and less computational power of IoT devices, complicated algorithms of cryptography cannot be used. Also, using and distributing the keys among a large number of IoT devices is a major obstacle. As the innovations in technology making cybercriminals perform more sophisticated attacks, security experts need to focus not only on the above features but to improve the security at the hardware level also. The more challenging issue is making the IoT devices to defend the new attacks [20].

B. Open Architecture:

As the Internet follows open accessing policies and providing data access to the public in a flexible way, the protocols and infrastructure of the Internet must be fair, autonomy and adaptive. This may lead to vulnerabilities as the cybercriminals are trying to exploit Internet users in many ways. Providing security on the Internet is one of the biggest challenges and it significantly considerable for the billions of IoT devices that are using Internet services.

C. Inadequate trust and integrity:

Attacks on IoT applications are mainly focusing on manipulating IoT devices. These devices will reach 50 billion in the near future and it is highly difficult to accumulate this huge number of devices under one monitoring section to provide regular security updates. This will increase the users' negative perspectives and this may lead to their unacceptance of IoT devices. The risks are more as one compromised device in an IoT network can give access to all other devices in the network. With more number of devices are connecting to the Internet, it is very much essential to ensuring the trust and integrity of every IoT device that is a part of the IoT application.

D. Lack of Standardization:

The main obstacle to standardize IoT devices is their availability in a number of varieties. Every device is like a standalone system with hardware, software, and protocols. One should incorporate security during the design and manufacturing phase of the devices. But there is no practical way of standardizing these devices. Even though NIST provides principles and practices for security in information systems, there is a lack of proving security for IoT [21]. And even they standardize the IoT, it is highly impossible to audit every IoT device due to their heterogeneity and enormous count.

E. Software Vulnerabilities:

As the operation of IoT devices requires less intervention of human beings, the software needs to be updated regularly and IoT devices must be configured to do so. Otherwise, the devices may be exposed to attacks. If the manufacturer discontinues the product then the devices may not get updates and they lack the technical support. If attackers find a way to get into the system, then they may leverage the device by running some arbitrary code and they may get authorization to control the device [22].

F. Targeting IoT devices:

Attacker shows more interest in IoT devices because of the devoid security features. Devices that are related to health care, surveillance, etc. are more targeted by hackers. As the validation and standardization of these devices are still in the beginning stage, malware can easily penetrate into these devices and can give access to the intend attackers.

G. Insecure web interfaces:

Attacks like account lock, brute force, and account enumeration may target the weak web interfaces to IoT devices. Attackers can login using a brute force attack and may change the administrative configurations and can access sensitive data. They may modify the credentials and make the system to disallow legitimate users. This risk is present in all IoT devices as the manufacturers assume the device will be accessed by the trusted users only.

H. Privacy Issues:

Protecting end users' privacy is more challenging as more IoT devices are collecting users' personal data. As big data technologies are evolving, the analysis of data on the Internet is becoming much easier even from large datasets. Obviously, this will endanger the privacy of many users.

I. Weakest Security Link:

Not like measuring security in normal applications, security in IoT is measured by finding the weak links. Because the more are the weak links, the more possibility for security breaches. Attackers will exploit these weak links, gain control of the devices and can access the data.

VI. REDUCING THE RISKS

In the earlier sections, we have discussed the challenges in providing security for IoT applications and this section deliberates some steps to reduce the risks in IoT security.

A. Security Policies:

Most of the existing security policies are helping to reduce the IoT applications security risks. By separating IoT devices from the core network and using virtual LAN if to maintain in core network can isolate the IoT devices during security breaches. Enforcing policies to limit data access, obscurity, and diversity should be adopted for IoT devices.

B. Identify, Locate and Track Devices:

A crucial part of ensuring security is locating and identifying the IoT devices in a network. Some devices are deployed in secure locations and some may not [23]. Devices that are in open locations can be easily accessible to the attackers and they can tamper the device and access the data. Physical layer attacks may happen on indoor placed devices by generating fake signals altering the location data. To counter these threats, relate the devices with intended applications and verify the identity before giving access to the device.

VII. CONCLUSION

This paper mainly analyses various issues related to providing security for Cloud-based IoT Applications. After discussing several recent works in this domain, the authors proposed a model to ensure security while transmitting data from IoT devices to the Cloud Storage Facility. Also deliberated various challenges and possible solutions to handle the risks that may affect the performance of IoT devices. As a future enhancement, we plan to enhance the model to focus on novel IoT attacks while en route the data to the Cloud Facility.

VIII. ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their valuable feedback. We would like to thank our Computer Science Department for providing the necessary resources for our work. This paper reflects the views only of the authors, and others cannot be held responsible for any use which may be made of the information contained therein

IX. REFERENCES

[1] "The Internet of Things : Vertical Solutions," *CISCO.com*, 2015. [Online]. Available: https://www.cisco.com/web/offer/emear/38586/images/Presentations/P11.pdf. [Accessed: 29-Sep-2018].

[2] "Unlocking the potential of the Internet of Things | McKinsey." [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. [Accessed: 09-Feb-2019].

[3] S. Workshop, C. Policy, and D. W. Regimes, "CISCO 2018 Annual Cyber Security Report," 2018.

[4] J. Levy, "Sophoslabs 2019 Threat Report," 2018.

[5] M. E. S. Elrabaa, "FPGA-BASED SYMMETRIC RE-ENCRYPTION SCHEME TO SECURE DATA PROCESSING FOR CLOUD-INTEGRATED INTERNET OF THINGS," *IEEE Internet Things J.*, vol. PP, no. c, p. 1, 2018.

[6] L. Peng, A. R. Dhaini, and P. Ho, "Toward Integrated Cloud-Fog Networks for Efficient IoT Provisioning : Key Challenges and Solutions," *Futur. Gener. Comput. Syst.*, 2018.

[7] B. Mukherjee *et al.*, "Flexible IoT security middleware for end-to-end cloud–fog communication," *Futur. Gener. Comput. Syst.*, vol. 87, pp. 688–703, 2018.

[8] E. Madeira, M. Curado, L. Villas, L. Silva, C. Lee, and O. Rana, "US CR," *Internet of Things*, 2018.

[9] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *J. Netw. Comput. Appl.*, 2018.

[10] F. Behmann and K. Wu, *Collaborative Internet of Things (C-IOT)*. 2015.

[11] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption," *Procedia - Procedia Comput. Sci.*, vol. 89, pp. 43–50, 2016.

[12] H. Geng, *Internet of Things and Data Analytics Handbook*. 2016.

[13] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and Privacy for Cloud-Based IoT : Challenges , Countermeasures , and Future Directions," no. January, pp. 26–33, 2017.

[14] C. Bodei, S. Chessa, and L. Galletta, "Measuring security in IoT communications," *Theor. Comput. Sci.*, no. December, 2018.

[15] M. Jia, S. Member, Z. Yin, S. Member, D. Li, and S. Member, "Toward Improved Offloading Efficiency of Data Transmission in the IoT-Cloud by Leveraging Secure Truncating OFDM," *IEEE Internet Things J.*, vol. PP, no. c, p. 1, 2018.

[16] C. Stergiou, K. E. Psannis, B. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Futur. Gener. Comput. Syst.*, 2016.

[17] "Google Cloud IoT - Fully managed IoT services | Google Cloud." [Online]. Available: https://cloud.google.com/solutions/iot/. [Accessed: 09-Feb-2019].

[18] "Windows 10 Internet of Things | IOT Devices | Microsoft." [Online]. Available: https://www.microsoft.com/en-us/windowsforbusiness/windows-iot. [Accessed: 09-Feb-2019].

[19] "Android Things | Android Developers." [Online]. Available: https://developer.android.com/things/. [Accessed: 09-Feb-2019].

[20] U. A., S. J., and K. S., "Embedded security for internet of things," *Proc. - 2011 2nd Natl. Conf. Emerg. Trends Appl. Comput. Sci. NCETACS-2011*, pp. 50–55, 2011.

[21] NIST, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, no. September. 1996.

[22] "MatrixSSL Vulnerabilities Expose IoT Devices to Attacks | SecurityWeek.Com." [Online]. Available: https://www.securityweek.com/matrixssl-vulnerabilities-expose-iot-devices-attacks. [Accessed: 09-Feb-2019].

[23] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari,

and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

Authors Profile

Mr. ***Raviteja Gaddam*** received B.Tech degree in CSE from Bapatla Engineering College and M.Tech degree in CSE from NIMRA College of Engineering & Technology. He is currently pursuing Ph.D. (CSE) at Pondicherry University. He received TCS Gold Medal for standing "Best Student of CSE&IT" during his B.Tech course. He qualified both SET & NET. He worked as a lecturer for three years at Bapatla Engineering College and as an Assistant Professor for six years in St. Mary's Women's Engineering College. His research interests include Network Security, Networking, Cryptanalysis, and Information Security. Currently, he is doing his research work on providing efficient intrusion detection in conventional and IoT networks.

Dr. M. Nandhini received B.Sc. and MCA degrees from Bharathidasan University, M.Phil degree from Alagappa University and pursued Ph.D. from Bharathiar University, Tamilnadu and qualified NET with lectureship. Currently, she is working as an Assistant Professor in the Department of Computer Science, Pondicherry University. She published more than 75 papers in various national and international conferences and journals. Her area of interests includes Evolutionary Algorithms – Soft Computing, Combinatorial Problem Optimization, Artificial Intelligence, and Software Engineering