Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models

Zeinab Bakhshi[1], Ali Balador[2,3] and Jawad Mustafa[2],
[1]RighTel, Iran, bakhshi.zeynab@gmail.com
[2]RISE SICS Västerås, Sweden, {ali.balador, jawad.mustafa}@ri.se
[3]Mälardalen University, Sweden, ali.balador@mdh.se

***Abstract*— This paper investigates security concerns and issues for Industrial Internet of Things (IIoT). The IIoT is an emerging transformation, bringing great values to every industry. Although this rapid alter in industries create values, but there are concerns about security issues, most of which would be still unknown due to the novelty of this platform. In order to provide a guideline for those who want to investigate IoT security and contribute to its improvement, this paper attempts to provide a list of security threats and issues on the cloud-side layer of IoT, which consists of data accumulation and abstraction levels. For this reason, we choose Cisco and Microsoft Azure IoT Architecture as reference models. Then, two layers of Cisco reference architecture model have been chosen to be investigated for their security issues. Finally, consideration of security issues has been briefly explained.**

I. INTRODUCTION

The Internet of Thing (IoT) has been firstly defined as a system of interconnected devices [1]. However, there is not a unique definition for IoT [2]. IoT named devices with smart interferences and identity that can connect and communicate to add value to their environment and users [3]. The scope of IoT application ranges widely in different areas, some instances are, smart homes, environment monitoring, health care systems, energy management, building automation and transportation. Application of IoT in industrial and manufacturing segments is known as Industrial Internet of Things (IIoT). This concept is also called industry 4.0 [4]. Leveraging IIoT will revolutionize factory and industrial segmentations by presenting its excellence. Far greater efficiency, accuracy, scalability, money saving, time saving, predictive maintenance and many other values are instances of IIoT benefits [5], [6]. However, the side effect of this emerging phenomenal (IIoT) has its own concerns for adaption. According to Gartner forecast, information security is a top concern among enterprises adapting IoT [7]. Security concerns would be barriers or major point of issue where things are responsible to control sensitive machinery and controlling systems in industries. Financial loss and confidential data leakage at least, death and injuries at most should be considered of the impact of security threats and cyber-attacks in IIoT. Studying IoT security threats in different application specifically in industrial segmentation is an ongoing research area in academic and industrial surveys. Therefore, in this survey we summarize IIoT security threats and security considerations. More particularly, this paper: (a) investigates previous works in IoT; (b) describes Cisco and Microsoft IoT Architecture as comprehensive reference models of IoT (c) summarize momentous security threats on two layers of Cisco and Microsoft reference models which has not been studied yet; and (d) review proposed security considerations that needs further research to address possible threats.

II. BACKGROUND AND STATE OF THE ART

Several survey papers have been studied to find out what has not been covered in the area of IoT security. We focused on papers that explicitly surveyed on security concerns in IoT. In these papers, different architecture models are considered and security threats are investigated and explored in different layers. Table I indicates a summary of studied papers. As it is shown in table I, there are different IoT architecture models, some papers discussed only one architecture and others discussed different IoT architecture models and deducted to present one model covering additional aspects of an IoT structure. Only 3 of them have focused on IIoT and its security concerns, however even in those papers IIoT in general was not the objective of the research and each had a focus on a specific application area, for instance, health care systems [8] or industrial data systems [4]. In this paper, we want to focus on IIoT without selecting any specific application area to cover common security concerns for different industrial areas. To achieve this, first we need to describe a comprehensive IoT architecture for IIoT. An Industrial solution demands an architecture that fits the IIoT applications. Such an architecture for instance should clarify and identify each process in IoT and also should support bidirectional data flow, real-time data collection and analysis. The reason is that the prevailing direction of data flow, data collection and data analytical needs differ in different industrial applications. As an instance in a command and controlling IoT system like door locking and unlocking data flow direction is from upper layers (application and users) to lower layers (edge side). However in a monitoring application like, fire fighting sensors data flow direction is from bottom to top and in some other applications like connected cars a bidirectional data flow should be considered. So next we describe proposed IoT architectures to come up with IoT architecture as a reference model that suits industrial needs.

TABLE I

A SUMMARY OF SURVEYED PAPERS

Row	Title	Year	Application Area	Cloud Focus	IoT Architecture	Layers Surveyed	Security Survey Area
1	A Comprehensive Study of Security of Internet of Thing[2]	2016	General	No	7 Layers, Cisco Reference Model	Layers 1, 2, 3 of Cisco Reference Model Edge Side Layers.	Security threats and countermeasures in 3 layers
2	Twenty security considerations for cloud-supported Internet of Things[9]	2015	General	Yes	3 Layers	Endpoint, Gateway and Clouds Layer	Security considerations in Clouds, Things, Fog
3	Cloud-assisted Industrial Internet of Things (IIoT)- enabled framework for health monitoring[8]	2016	Health Care Monitoring	Yes	4 Layers	Things and Clouds Layer.	Signal monitoring in Health-care application
4	Internet of Things(IoT): Security Challenges, Business Opportunities and Reference Architecture for E-Commerce[10]	2015	E-Commerce	No	E-Commerce Scenario	IoT Challenges in General	IoT challenges in general
5	Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures [11]	2015	General	No	3 Layers	Perception, Network and Application Layer.	Security threats and countermeasures in 3 layers
6	Mitigating loT Security Threats with a Trusted Network Element [12]	2016	General	No	4 Layers	Perception , Network, Middle Ware and Application Layer.	Security threats and countermeasures in 4 layers
7	The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing and Other Computational Intelligence (EC&CI) [4]	2016	Industrial Data Systems	No	1) 6 Layers 2) 4 Layers 3) 5 Layers	1) General Survey on Different Infrastructures 2) Cisco Old IoT Framework	Security challenges in EC & CI, Data Mining, Big Data
8	Security and Privacy for Cloud-Based IoT: Challenges, countermeasures, and Future Directions [6]	2017	General	Yes	3 Layers	Sensing, Network and Application Layer.	Authentication, Privacy Encryption, Packet Forwarding
9	Internet of Things: A Survey on Enabling Technologies,Protocols and Applications [13]	2015	General	No	5 Layers	Object, Object Abstraction, Service Management, Application and Business Layer.	Security protocols in IoT
10	A Critical Analysis on the Security Concerns of Internet of Things (IoT) [1]	2015	General	No	4 Layers	Perception , Network, Middle Ware and Application Layer.	Security threats and countermeasures in 4 layers
11	End-to-End IoT Security Middleware, for Cloud-Fog Communication [14]	2017	General	Yes	3 Layers	IoT Nods, Middle Ware and Gateway Layer.	Security threats in 3 layers
12	A Scalable and Manageable IoT Architecture based on Transparent, Computing [15]	2017	General	No	5 Layers	End-user, Edge network, Core network, Server & Storage and Management Layer.	--
13	A Survey on IoT Architectures, Protocols, Applications, Security, Privacy, Real-World Implementation and Future Trends [16]	2015	General	No	5 Layers	Perception, Network, Middle Ware, Application and Business Layer.	Security challenges, Privacy

A. IoT Architecture

There is a basic IoT architecture model, which is used by many papers in the literature on IoT security. This basic model is a 3-Layered architecture model driven from wireless sensor network concept [2]. The 3-Layered architecture model has been improved with more abstraction in some other papers with 4 and 5-Layered architectures, however, none of these basic models can address IoT functionalities and operations of industrial IoT [17]. A real-time business solution needs an architecture to collect, analyze and share data [18]. Such an architecture for IoT solutions demands cloud services to authorize device, ingest data, data integration and aggregation, stream processing, advanced analytics, and most importantly secure storage and identity services plus users roles definitions [18]. Cisco and Microsoft each provides an IoT reference architecture for such solutions known as Cisco IoT Reference model and Azure IoT Suit Architecture, respectively. Azure IoT Suit architecture supports heterogeneous devices. Devices can have direct connection however a gateway based architecture enables a more secure approach in IoT architecture. The architecture guides to enable and validate security among all component which includes authentication of device and users, data encryption for data at rest and data in motion [19]. Cisco IoT Reference model describes how tasks at each level should be handled to maintain simplicity, allow high scalability, and ensure supportability. This model defines the functions that required for an IoT system to be completed [17].

To the best of our knowledge and as it is shown in Table I, only one of the papers used Cisco reference model as IoT architecture and investigates security concerns and their countermeasures. But, it has been focused on the first three layers, edge computing part, of the Cisco IoT Reference model. Cisco IoT model has been used as a reference model in this survey. Table II shows different IoT architectures and their relationships. Cisco architecture is the reference model here in this table and other architectures are compared to the layers in Cisco model. Azure IoT architecture is not a layered model and includes services or components, but we tried to map it to the Cisco reference model. Grey background boxes represent layer 4 and layer 5, which will be the focus of this paper.

III. SECURITY CONCERNS

In this section we approach to deliberate security challenges and possible threats at layer 4 and 5 of Cisco architecture model. Figure 1 summarize studied security threats

TABLE II
DIFFERENT IOT ARCHITECTURES

Cisco Levels	3 Layered	5 Layered	Cisco IoT Architecture (7 Layers)	Azure IoT Architecture (3 Groups)
7	-	Business	Collaboration & Processes	Cloud Visualization & Integration
6	Application	Application	Application	Cloud Data Processing Services
5	-	-	Data Abstraction	Cloud Data Storage Services
4	-	-	Data Accumulation	Cloud IoT Data Ingest Services
3	-	Middleware	Edge/Fog Computing	-
2	Network	Network	Connectivity	Connectivity
-	-	-	-	IoT Gateway
1	Perception	Perception	Physical Devices (Perception)	IoT Devices

and vulnerabilities in layer 4 and 5. Then in the next section security considerations for each layer will be discussed.

A. Security Concerns in Cisco IoT architecture

1) Data Accumulation Layer: The main task of this layer is to convert data format from data packets to database tables [2]. Transition from event based to query based computing and reducing data through filtering are other tasks in this layer. Network datasets in repositories should be converted in a form that can be used by application layer. For this reason, event based data will be converted to query based data and get compressed and filtered to be utilizable for abstraction and application layers. Data, storages, execution algorithm and patterns are the properties and quiddity of this layer. Some common attacks against this layer are studied as below:

- Metadata Spoofing: This type of attacks occurs when the attacker changes or modifies the files of database instances. It causes an interruption in service and makes data unreliable and unavailable [20][21]. In an IIoT context an intruder might be able to modify database and cause data integrity be compromised. It helps the attacker use system errors to bypass authentication and access target data.
- SQL Injection: in this kinds of attacks, the attacker tries to enter Structured Query Language (SQL) commands to steal contents within a database. SQL injection can be branched into other types of attacks like, (a) Authentication Bypass. (b) Information Disclosure, (c) Compromise Data Integrity, (d) Compromised Availability of Data, (e) Remote Command Execution [21][22].
- Resource Exhaustion: this is a kind of vulnerability caused by bad design or inefficient implementation or resource leakages [23]. There seems to be a large number of components in an integrated IIoT system each of them needs computing resources. data communication, data storing, process management and etc. all need resources to be operate as required in a system. If the system lacks resource or resource distribution management, an attacker can intrude IIoT system and cause data integrity and availability be compromised.
- Ransomware: this type of attacks are denial of access attacks, using malwares or malicious code injection to hostage target data using cryptovirology techniques until the requested ransom is fully paid. MacAfee, strongly stated that Ransomware will readily migrate to IoT [24].
- Malicious Attack: in this type of attacks a malicious insider or intruder attempts to launch an attack to exploit a service or data. This can be performed by leveraging other methods like phishing, IP spoofing, DNS poisoning attacks or malicious injection. The malicious attacker captures and analyzes data available in an IoT system to launch DoS or DDoS attacks [25][9][20].

2) Data Abstraction Layer: In this layer, Information and multiple data from different systems are integrated. As instance, data from ERP, CRM, IoT devices and other sources are combined and filtered and reconciled. Integrating data from multiple sources, shaping data, creating data scheme for application layer are tasks of this layer. Data, Information, Access protocols and their semantics and aggregation for analytical purposes are the properties and nature of this layer.

- DDoS: Distributed Denial of Service is a wide rage DoS where multiple systems that are mostly infected by malwares are used or abused to lunch the attack and target the victim system. Due to DDoS availability and integrity of sensitive data is compromised and users of the system cannot access legible data. As instance in an IIoT system a fire detection sensor sends data but the system is out of service due to a lunched DDoS attack and this cause a disaster [26][27][28].
- Man in the Middle (MitM): this attack involves an attacker to place in a communication channel while data is transferring between two parties of link. Confidential information like authentication data (username, password), addresses, massage contents and all manners can be leaked through this attack [29][25].
- Replay Attack: in this type of attacks the attacker aims to capture a legible sequence of an authentication session by an authorized user then replays the same request and get access to sensitive data as plain text format [30]. Multiple components in an IIoT need to be authenticated to access data for instance, devices, routers, users therefore the attacker have more opportunity to compromise the system capturing a legible access and running the attack consequently.
- Brute Force: In this attack the adversary aims to find legible credentials to access the database. To achieve this the attacker uses exhaustion methods to do trial and error to find out a legible access or decode encrypted data [31].
- Buffer Overflow: this refers to a type of anomaly that

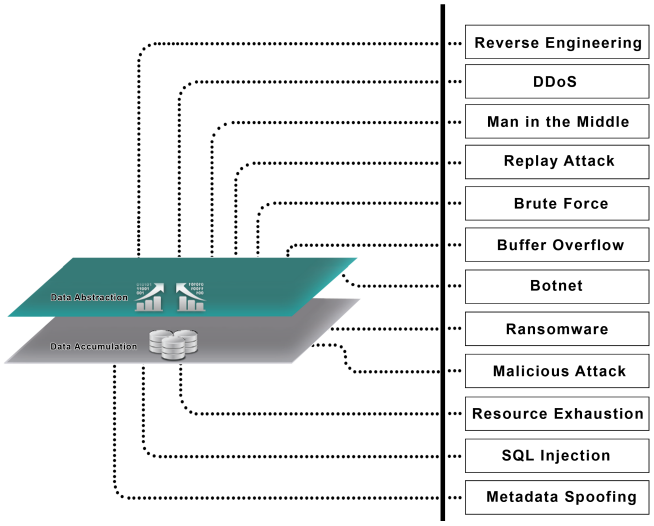

Fig. 1. Summary of security threats within layer 4 and 5

a process or program tries to write or overrun data in a buffer memory. Attackers use buffer overflows to interrupt execution of system codes and run arbitrary commands to take over a system or database information [31].

- Botnet: A botnet is a robot network of compromised machines, or bots, that run malicious software under the command and control of a botmaster [32]. one of the most famous examples of Botnet is Chikdos [33]. This attack malware targets database services mostly MySQL servers to lead them lunch a DDoS attack against other services.
- Reverse Engineering: In data aggregation, reverse engineering helps the attacker search the reverse data and object they need by searching the opposite data labeled as negative hence they can find and access true data by finding all the others classified objects and reversing them [34].

B. Security Concerns in Azure IoT architecture

1) Cloud IoT Data Ingest Services:

- Nefarious activity and abuse such attack is made on infrastructure to damage a business or reputation of community [35]. If IoT architecture is highly distributed, then significance of such attacks increases. Low level threats of which are Identity theft, DoS, DDos, Malicious Code, Social Engineering.
- Eavesdropping, interception and hijacking communication these are like man-in-the-middle attacks and such attacks can reduce data collection and it can affect data-in-motion [35]. Interception of Information, Relay of massages and MitM are the attacks of this high level threat.
- Tampering a data interception can lead to data tampering which is even more critical attack because an attacker can send false data and it can change the whole business process [36]. For example, false alarms or invalid messages that effect data aggregation.

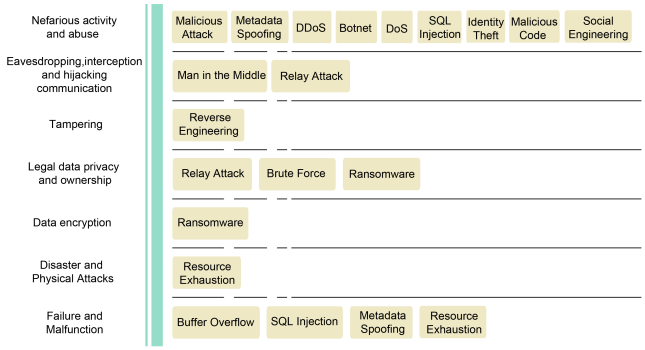

Fig. 2. Security threats classification

2) Cloud Data Storage Services:

- Legal data privacy and ownership is a big challenge, and it can create big impact on business and government if legal actions or orders mismatch IoT architecture [35]. Brand damage and financial loss are the consequences of this high level attack.
- Data encryption and FIPS compliance data encryption requirements can vary for different businesses. If a business has specific encryption requirements like FIPS compliance then a storage not supporting such encryption can cause problems [37].

3) For Both IoT Data Ingest and Data Storage Services:

- Disaster and Physical Attacks any disaster on physical storage of data can result in huge data loss. Such attacks can be result of intentional, natural or collateral damages [35].
- Failure and Malfunction failure or bugs of software services can create disrupt in IoT architecture. Such failures and bugs can be caused by design issues or testing errors of software development process.

In order to summarize security concerns related to storages and data access in an IIoT architecture, we used security threats and concerns mentioned by Microsoft for Azure IoT architecture as a reference and security threats that we mentioned for Cisco architecture were assigned under those categories. There are clearly many other security concerns and issues to resolve related to storages and data access layers, however we approached to name some security concerns that need further research in IoT and IIoT context. Figure 2 shows the summary of threats, considering both Azure IoT and Cisco architecture.

IV. Approaches to Securing IIoT

Many researches have already focused on securing the things (devices) [2] [12]. But, securing things with encryption algorithm and authentication control systems is not capable of ensuring the whole data flow of IIoT. Data of things traffic through the whole IIoT architecture layers and not limited to device and fog layers. In this section, we briefly

describe security considerations that require further research in the context of large scale IIoT data flow and need to be thought before implementing an IIoT system in Layer 4 and 5 of IIoT architecture.

A. Communication Management

There is a bidirectional data flow in Cisco Reference model [17]. The industrial data is sensitive and this flow of data and data communication between layers is very important to be secured. Secure communication prevents data confidentiality and integrity adversaries and prevents data leakage and manipulation attacks like man in the middle, eavesdropping and other vulnerabilities against data communication channels. Transport Layer Security (TLS) and other mechanisms and encryption tools protect data in communication channel, however on April 2014 a vulnerability that allows stealing data protected under TLS was discovered hence, more observation and attention is required to support IIoT mass data communication [38][39].

B. Access Management

A crucial aspect of implementing data storages and communication is controlling and managing accesses to data objects. Performing data query, computation, changing and updating data objects require to be managed and regulated. Controlling data access needs considering two main factors, Authentication and Authorization management. The existing credential services, access control tools and policy defining components should be improved to operate far stronger. In an IIoT environment each device, end-user, process, application and so forth is known as users and should be authenticated and rules of authorization of which should be regulated for each component in order to prevent intruders to access data or do malicious modifications [40].

C. Data Encryption

Cryptographic methods is required for protecting sensitive data against attacks. Encrypting device codes, data in storages, data prepared to use in processes and for other layers ensures that data has not been tampered. There are many encryption algorithms and methods, however encryption of a large amount of data in IIoT, that come from different sources and need to be computed in a fraction of time required new methods of encryption and cryptography [2]. Using encryption increases memory usage, energy consumption, delay, and packet loss. There has been proposed different IoT encryption methods, for example, CLEFIA [41], PRESENT [42]. However, to the best of our knowledge, promising public key encryption methods that provide enough security while meeting lightweight requirements is still one of top security challenges in IoT [43].

D. Load Management

Service elasticity has been the aim of traditional storage and database designs to fulfill end-users or clients requirements. In an IIoT, the clients of a service are both the things and end-users. Therefore, both number of service users and the volume of data generated by them will be a concern for implementation. Resource expansion is not unlimited and the unknown peak of IIoT data should be managed before the unavailability concerns like DDoS or Resource Exhaustion happens [9].

E. Data Audit

Auditing is a relevant solution to verify data, ascertain information rules and regulation and protect services against data leakage, misconfiguration, malwares and tampers in data driven services. Tamper resident and hardware based cryptographic tamper proof products are the solutions to defeat data leakage, reverse engineering and misconfiguration, however a fit to IIoT platform scale improvement that can ensure all related security aspects is required. In an IIoT platform trustworthy audit services should be considered to assure the IIoT is performing as it is designed and regulated [9].

F. Data Combination

There are different privacy and security concerns for sensitive information gathered and aggregated from different sources in an IIoT platform. Data combining considerations should be thoughts to avoid privacy violence in aggregated data. This help to limit the risk of revealing sensitive information in data pool. Although privacy preserving and statistical disclosure control techniques have aimed to identify each single records, it is still difficult to prognosticate data leakage problems from data combining [44].

V. CONCLUSIONS

Apart from benefits that IoT brings in industrial segment, it creates an attractive opportunity for adversaries to attack, steal data, deny operation or causing broad damages to industries. In this paper, we attempted to survey as many IIoT security concerns and issues as possible and provided possible consideration for them. We focused on Cisco and Microsoft Azure reference models and especially data accumulation and abstraction layers, which has never been explored for their security concerns. We discussed possible security challenges in these layers for both Cisco and Azure architecture models and then we did a segmentation of threats based on security vulnerabilities and attacks. Finally, we discussed security considerations for all mentioned security challenges.

REFERENCES

[1] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1–6, 2015.

[2] A. Mohsen Nia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 6750, no. c, p. 1, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7562568/

[3] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 10–16, 2017.

[4] H. He, C. Maple, T. Watson, A. Tiwari, J. Mehnen, Y. Jin, and B. Gabrys, "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," *2016 IEEE Congress on Evolutionary Computation, CEC 2016*, pp. 1015–1021, 2016.

[5] IIoT. [Online]. Available: inductieautomation.com

[6] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[7] Gartner, forecast: Iot security, worldwide, 2016, available at. [Online]. Available: https://www.gartner.com/doc/3277832/forecast-iot-security-worldwide-

[8] M. S. Hossain and G. Muhammad.

[9] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, 2016.

[10] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*, pp. 1577–1581, 2015.

[11] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, pp. 336–341, 2016.

[12] J. Kuusijarvi, R. Savola, P. Savolainen, and A. Evesti, "Mitigating IoT security threats with a trusted Network element," *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*, pp. 260–265, 2017.

[13] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[14] B. Mukherjee, R. L. Neupane, and P. Calyam, "End-to-End IoT Security Middleware for Cloud-Fog Communication," *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, pp. 151–156, 2017.

[15] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, "A scalable and manageable IoT architecture based on transparent computing," *Journal of Parallel and Distributed Computing*, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.jpdc.2017.07.003

[16] M. Aazam and E. N. Huh, "Fog computing and smart gateway based communication for cloud of things," *Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014*, pp. 464–470, 2014.

[17] J. Green, "The Internet of Things Reference Model," *Internet of Things World Forum*, pp. 1–12, 2014.

[18] B. Familiar and J. Barnes. Business in real-time using azure iot and cortana intelligence suite.

[19] Microsoft azure iot reference architecture. [Online]. Available: https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available

[20] K. Munir and S. Palaniappan, "Security Threats / Attacks Present in Cloud Environment," *International Journal of Computer Science and Network Security*, vol. 12, no. 12, pp. 107–114, 2012.

[21] M. Jensen, N. Gruschka, and R. Herkenhöner, "A survey of attacks on web services: Classification and countermeasures," *Computer Science - Research and Development*, vol. 24, no. 4, pp. 185–197, 2009.

[22] Cisco knowledge base. [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/sql-injection.html

[23] J. Antunes, N. F. Neves, and P. Verissimo, "Detection and prediction of resource-exhaustion vulnerabilities," *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*, vol. 27513, pp. 87–96, 2008.

[24] I. McAfee, "McAfee ® Labs 2014 Threats Predictions," no. November 2016, pp. 1–6, 2014. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf

[25] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, no. December 2016, pp. 10–28, 2017.

[26] M. M. Alani, "Securing the Cloud: Threats, Attacks and Mitigation Techniques," *Journal of Advanced Computer Science and Technology*, vol. 3, no. 2, pp. 202–213, 2014. [Online]. Available: www.sciencepubco.com/index.php/JACST

[27] P.-L. D. Elike Hodo, Xavier Bellekens, Andrew Hamilton, C. T. Ephraim Iorkyase, and R. Atkinson, "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System," *2016 3rd International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1 – 6, 2016.

[28] A. Y. Nur and M. E. Tozal, "Defending Cyber-Physical Systems against DoS Attacks," *2016 IEEE International Conference on Smart Computing, SMARTCOMP 2016*, pp. 8–10, 2016.

[29] M. Johnson, *Cyber Crime, Security and Digital Intelligence*. Routledge, 2016.

[30] P. B. Rane, "Authentication and Authorization : Tool for E- Commerce Security," vol. 2, no. 1, pp. 150–157, 2012.

[31] S. T. Ahmed and N. Rahul, "Analysis of Security Threats To Database Storage Systems," vol. 3, no. 2, pp. 18–23, 2015.

[32] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[33]

[34] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of machine learning," *Machine Learning*, vol. 81, no. 2, pp. 121–148, 2010.

[35] Evaluating your iot security, microsoft azure. [Online]. Available: https://www.microsoft.com/en-us/internet-of-things

[36] Iot security architecture, threat model and iot security. [Online]. Available: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture

[37] Azure storage security guide. [Online]. Available: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

[38] (2014, apr) Heart bleed bug. [Online]. Available: http://heartbleed.com/

[39] Z. Durumeric, M. Payer, V. Paxson, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, and J. Beekman, "The Matter of Heartbleed," in *Proceedings of the 2014 Conference on Internet Measurement Conference - IMC '14*, 2014, pp. 475–488. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2663716.2663755

[40] S. Misra and A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks," *Computer Communications*, vol. 34, no. 3, pp. 281–294, 2011.

[41] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, I. T. Shirai Taizo, Shibutani Kyoji, Akishita Toru, Moriai Shiho, T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-Bit Blockcipher CLEFIA (Extended Abstract)," *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, vol. 4593, pp. 181–195, 2007. [Online]. Available: http://www.springerlink.com/index/10.1007/978-3-540-74619-5

[42] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT : An Ultra-Lightweight Block Cipher," *Springer Berlin Heidelberg*, pp. 450–466, 2007.

[43] M. Katagi and S. Moriai, "Lightweight cryptography for the Internet of Things," *Sony Corporation*, pp. 7–10, 2008. [Online]. Available: http://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

[44] C. Dwork, "Differential Privacy: A Survey of Results," *Theory and Applications of Models of Computation*, pp. 1–19, 2008.