Security Frameworks for Internet of Things Systems – A Comprehensive Survey

Conference Paper · August 2020

DOI: 10.1109/ICSSIT48917.2020.9214127

2 authors:

Vadiraja Acharya
PESU
4 PUBLICATIONS **13** CITATIONS
SEE PROFILE

Vinay V Hegde
Rashtreeya Vidyalaya College of Engineering
13 PUBLICATIONS **65** CITATIONS
SEE PROFILE

Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

Security Frameworks for Internet of Things Systems – A Comprehensive Survey

Vadiraja Acharya*, vadiraja.a@jyothyit.ac.in
*Research Scholar, VTU, India

Vinay V Hegde**, vinayvhegde@rvce.edu.in
**Computer Science & Engineering Department, RVCE, Bangalore, India

***Abstract*—Security frameworks are playing an important role in building a robust IoT system. IoT as understood today has the challenge of varied standards, architectures and models by referring the corporate that develops different applications. But, to evaluate and benchmark the security aspects of the designed IoT application, a single methodology cannot be followed, as each of those are developed based on a different architecture. Hence, a survey is undertaken to study all the security frameworks proposed by researchers, industry and those which are just conceptual. This paper discusses about various IoT architectures, security attacks possible on layers, protocols and devices of an IoT system and finally a comprehensive survey is performed on all the security frameworks of IoT systems. Further, they are classified based on the focus or the thrust area in developing the same. Finally, this survey work is concluded by comparing the security frameworks based on few important metrics and by suggesting the required improvements in designing a generic security framework that handles majority of shortcomings in the present frameworks and practices.**

Keywords – IoT; security frameworks; IoT architecture; IoT security attacks

I. INTRODUCTION

Internet of Things in recent times has attracted enough attention of researchers, academicians and industries as it is uncovering new potential of knowledge and economy respectively. Connecting anything and everything to the fabric of Internet is making it easy to build exciting applications and bring value to the unexplored data that was previously collected and never used. Businesses are using IoT to a) increase productivity b) generate new revenue streams c) enhance regulation compliance and d) improve customer loyalty [1]. Examples for each of these can already be seen in the market. Connected machines are harvesting the daily usage for predictive maintenance, livestock management, smart metering and in-car connected devices for fleet tracking, etc[1]. However, all the above mentioned applications of IoT need to be built securely, failing which any device could be used to launch an attack on desired target.

According to this report [1], IoT threat landscape is large and growing, hence well-designed IoT security architectures are required by companies and organizations for adopting IoT technologies. It also mentions that it is not trivial to have a single architecture that can serve as a blueprint for all verticals of IoT applications. Considering the components of any IoT application, the physical devices, edge and the platform has to be built securely to thwart possibilities of attack on them. In [2] the authors discuss the shift in the IoT security architectures from three-layered to four-layered, cloud computing to fog computing, edge to Blockchain based architectures. Security frameworks for IoT applications are as crucial as security architectures which are just conceptual. However, there is no silver bullet which serves as a common framework for all possible applications in various verticals. A security framework should consider all types of security attacks possible on each of the layers in the IoT architecture. Devices in the Perception layer, Protocols used to connect these devices to the middle-ware, Application interface used to manage these devices and the data generated out of these, are all the aspects which should be considered.

The goal of this paper is to provide a comprehensive consolidation and classification of all the available security frameworks for IoT applications. We also provide a survey of different IoT architectures suggested by various consortium, possible security attacks on the IoT devices, network and middle-ware. Further we compare all the security frameworks based on important metrics like, type, focus area, implementation, test-bed setup and results. Lastly, we provide a list of improvements based on the current study to design a robust system.

The remainder of the survey paper is organized as follows. In Section II, we present a systematic survey of IoT architectures and shifts in paradigm. Following that, in Section III, we present a short survey on security attacks on IoT layers. Next in Section IV, we conduct a detailed survey on Security Frameworks for IoT systems. Finally in Section V we compare each of them and conclude.

II. IoT ARCHITECTURES

Various multi-layered architectures are proposed like Three-layered [3] as shown in *Figure–1* , Four-layered [4], Five-layered [5]. Other recent ones proposed include, Service Oriented Architecture (SOA) [6], Work done in [16] compares the Cloud Architecture [7], Fog Architecture [8], Edge Architecture [9] and Mist Architecture [10] specific to IoT.

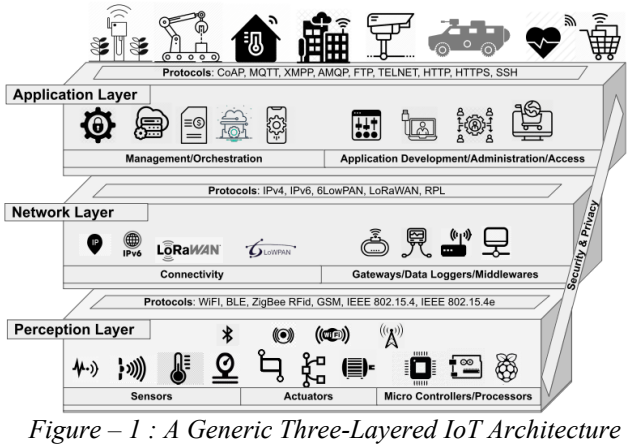

Figure – 1 : A Generic Three-Layered IoT Architecture

This work here [13] presents an extensive survey of all types of IoT architectures prevalent in the industry. It provides three perspectives to IoT architecture designs a) X-Centric approach, X means, focus on a particular element of the IoT system such as a Gateway or User, b) System viewpoint which centers on a particular slice of the full IoT system, such as a cloud, finally c) The universal approach, which addresses all elements of the stack (End-to-end comprehensive architecture). Further it also talks about IoT Middle-ware Architecture, Data-Centric Lambda Architecture. Other reference models, the work [13] talks about are the generic IoT-A RA by European Lighthouse Project in 2010, ITU-T Y.2060 IoT Reference Model, IoTWF (World Forum) Reference Model, OneM2M RA, which is a horizontal platform architecture to exchange data between applications, IEEE P2413 IoT Architecture which promotes cross-domain interaction and facilitates system interoperability with functional compatibility[13], OpenFog Consortium Reference Architecture based on eight pillars including Security, Scalability, Open, Autonomy, RAS, Agility, Hierarchy and Programmability [13]. Then it talks about the Alliance for the Internet of Things Innovation (AIOTI) WG03 IoT Reference Architecture, There is another open source reference implementation called interconnectivity from the open connectivity foundation [13]. There are multiple groups, which focus on a particular domain, industry or market, like The Industrial Internet Consortium (IIC) which suggests an IIC Reference Architecture Three-Tier Pattern, OPC Unified Architecture (OPC UA) is another one which is a platform-independent service-oriented architecture [13]. More recently, industries have shown interest in leveraging Network Function Virtualization (NFV) [14] and Software-Defined Networking (SDN) [15] for IoT, they have been proven to scale, orchestrate, automate and provide reliability for IoT implementations. Latest work presented here [11] modifies the existing Three-Layered architecture for Real-Time Machine Learning capabilities.

In another work [12] Software Engineering concepts of Architectural Styles are introduced for IoT applications. There are specific architectures suggested for a particular application domain like [17] & [18] where the authors talk about approaches to build Smart City and Healthcare applications respectively.

With a host of such architectural approaches available today, choosing the right one is a major challenge for any organization. However, combining this with Security built in from the ground up should be a minimal requirement for any business to adopt the same.

III. SECURITY ATTACKS ON IoT

Multiple surveys have been conducted detailing all possible attacks on the IoT stack. They have also suggested mitigation techniques and applied Blockchain for same. Most recent work [19] provides a detailed survey and Taxonomy of attacks on IoT applications and various layers of IoT architecture. An earlier work [20] provides the countermeasures for all the attacks based on the security requirements like Confidentiality, Integrity, Availability, Accountability, Auditability, Trustworthiness, Non-repudiation and Privacy. However, each of these works mentioned have considered either the three-layered or four-layered general IoT architectures for study.

A work in [2] conducts a survey on the security issues of Cloud, Fog, Edge, SDN and NFV architectures. It also suggests Machine Learning based security approaches to mitigate the attacks.

In an another work here [21], apart from surveying the possible attacks, it also discusses a Three-layered IoT security architecture, further it lists the tools that are used to simulate and analyze each of the attacks. Open Web Application Security Project (OWASP) is a foundation which works towards improving security of software by providing tools and resources to its community. It lists all the possible attack vectors on three-layered IoT system. It includes the attacks on Hardware (Perception Layer), Communication Link(Network Layer) and Interfaces/Services (Application Layer). Hence, IoT security architecture should encompass all the mitigation techniques to secure the IoT system built on any IoT architecture discussed in Section II.

A comprehensive study on security attacks with test-bed setup and mitigation techniques are discussed here [22]. It also talks about the security issues of NB-IoT and suggests solutions using Blockchain. Based on all the previous works mentioned till now, Table-1 summarizes the vulnerabilities which causes different attacks on IoT systems leading to breach in security principles[19][20][21][22].

Table – 1: Vulnerabilities & Attacks

Security Principles	Attack	Vulnerability
Confidentiality	> Monitoring Attack > Traffic Analysis Attack > Man In the Middle > Unauthorized Access > Spyware > Adware > Data Breach > RFID Spoofing	> Device Scanning > Brute force > Device Spoofing > Voice Squatting > Voice Masquerading > Poor design choice > Buffer overflows > Improper Exception Handling > Weak Passwords > Lack of Multi-factor Authentication
Integrity	> Message Alteration > Message Fabrication > Incorrect Data Injection > Data Inconsistency	> Poor design choice > Buffer overflows > Improper Exception Handling
Availability	> DoS/DDoS > Malware > Virus >Black-hole > Wormhole > Broadcast Tampering > Spamming > Fake Node Injection > RF Interference > Sleep Denial Attack > Side Channel Attack > Routing Information > Replay Attack > Sybil Attack	> Weak Cryptographic Algorithms > Weak security parameters >Weak Configuration setting > Replace device firmware > Software Reverse-engineering for cloning > Poor design choice > Buffer overflows > Improper Exception Handling > Weak Passwords > Lack of Multi-factor Authentication > SQL Injection

Year-on-year different studies have proven that number of security attacks on IoT systems have increased steadily. Symantec reports [23] a 13% increase in the attacks on its IoT Botnets which emulate protocols used by almost all IoT devices such as routers, connected cameras, digital video recorders etc. It has also reported a fall in the number of IP addresses used to launch the attacks, which infers more

aggressive IoT Botnets. Further it also lists the top ten easily guessable passwords of IoT devices which are used by the attackers to gain access. *Table – 2* lists multiple attacks on IoT systems in reality this decade.

Figure-2 shows the number of attack events on TCP ports of IoT honeypots in the first half of year 2019 according to [52]. We can clearly see that, protocols like Telnet which runs on port number 23 is the most attacked. We can infer that, attackers are using the vulnerability of weak passwords that are set in IoT nodes to get escalated privileges. Once they get it, that IoT node is converted into a DDoS node by a malware. The next most attacked port number is SMB (Server Message Block) running on port number 445 for file sharing services to push malware or even malicious code etc.

IoT stack has multiple protocols and each of them have security features built in by design. However, not all the protocols in the stack are secure by design. Multiple works have exposed the security flaws in these protocols.

In a work here [32] security vulnerabilities of BLE (Bluetooth Low Energy) are discussed with practical demonstration of attacks like spoofing, man-in-the-middle.

Security vulnerabilities of ZigBee protocols has been explored in this work [33] by looking at the ZigBee built-in security services, encryption techniques, security keys, and the trust center.

Table – 2: Lists of Security Attacks on IoT systems in reality

Year	Attack	Vulnerability
2015	Vtech Educational Toys exposed personal data of over 6 million users [24]	> SQL Injection > Un-encrypted Communication for account registration.
2016	Multiple DDoS attacks on DNS provider Dyn causing service disruption in Europe and North America [25]	> Mirai botnet exploited various vulnerabilities in 600,000 Internet-Connected devices to launch DNS look-ups.
	DDoS attack on websites like Krebs on security [26]	
2017	St. Jude's cardiac devices hacked to deplete the battery, administer incorrect pacing or shocks [27]	> Unauthorized access to device and modification to firmware.
2018	Hackers exploit casino's smart thermometer to steal database info [28]	> Weak encryption algorithms used for passwords.
2019	IoT malware called Silex used to wipe device firmware [29]	> Gained access via default credentials the device is shipped with.
2020	Trifo smart vacuum with vulnerabilities was presented as a target for remote attacks, including DoS and camera hacks. [30]	> Multiple undisclosed vulnerabilities in Camera and Firmware.
	A drone hacked Phillips hue smart bulbs and set a virus-like reaction. [31]	>Vulnerabilities in the ZigBee Protocol

In the work here [34] vulnerabilities of WiFi enabled drone has been analyzed by launching various attacks like denial-of-service, de-authentication methods, man-in-the-middle, unauthorized root access and packet spoofing attacks.

Authors of [35] have analyzed the LoRa network stack and discuss the possible susceptibility of LoRa devices to different types of attacks using commercial-off-the-shelf hardware. In [36] authors of have accessed the vulnerability of rank property in RPL(Routing Protocol over Low power and Lossy network)-6LoWPAN(IPv6 over Low-power Wireless Personal Area Network) protocols based on attack graph.

Further the work [37] carries out security analysis of CoAP (Constrained Application Protocol) along with suggestions of solutions to mitigate the same. Analysis of security in MQTT (Message Queuing Telemetry Transport) communication protocol has been discussed in [38] by demonstrating the attack scenarios.

By this discussion above, what can be inferred is every layer in the IoT stack has set of protocols which can be used to exploit the IoT system. Few are vulnerabilities generated out of poor protocol design or limitations of the protocols. Few other protocols can be exploited by gaining escalated privileges through non-standard practices. Host of other protocols which are part of the IoT stack are also discussed in many other works.

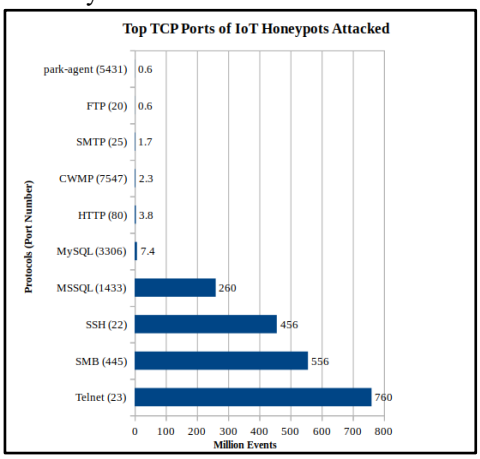

Figure – 2: Top TCP Ports of IoT Honeypots Attacked [52]

IV. SURVEY ON SECURITY FRAMEWORKS

Security Frameworks are the actual implementations of security architectures and play an important role in implementation of an IoT system. It can either make the system robust or prone to security attacks. Based on the survey of the available security frameworks, we can classify them broadly as follows, a) Application Specific b) Functionality/Protocol Specific c) Generic Frameworks. *Table – 3* shows the classification of security frameworks surveyed and their references.

Table – 3: Types of IoT Security Frameworks

Security Framework Type	References
Application Specific	> SAFIR: For Smart buildings [39] > PGFit: Health & Fitness app (Google Fit) [40] > For IIoT Applications [41]
Functionality/Protocol Specific	> Identity Management [42] > Security Policy Enforcement [43] >TruSD: Service Discovery at Edge [44]
Generic	> IoTSAT (Security Analysis) [45] > Privacy-By-Design [46] > Sensor to Cloud Ecosystem [47] > Mobility-First IoT Systems [48] > Industry Security Frameworks Survey [49] > SODA – Software Defined [50] > IoT Device Specific Framework [51]

Application Specific Security Frameworks are those which are designed for a particular use case. In [39] authors proposes a security framework specifically for smart buildings use case called SAFIR.

Table 4. Comparison of Security Frameworks for IoT Systems

Framework [Reference]	Type	Focus Area	Methodology &Implementation	Test-Bed Setup	Results	Lacuna/Limitations
SAFIR [39]	Application Specific	Authentication &Authorization	Authentication and Access Control Policy Specification based on OSGi (Open Services Gateway initiative) >mDNS >CoAP >CoRE-RD >JSON >XACML >Elliptic Curve Cryptography	>Intel Core i5, 4GM RAM (User) >Intel Zeon 4GM RAM(Security Components) >JN5148 Motes on Contiki OS	Delay measurements of, >Service Discovery >Authentication >Authorization	>No mention of Attack Scenarios on Authentication and Authorization process >Other Security Principles are not handled.
TruSD [44]	Functionality Specific	>Service Discovery >Trust	Simulation of Service Discovery based on Python implementation of, >Threat Model >Service Discovery Protocol	PC which has 8 GB RAM and Intel Core i7-3610QM 2.3 GHz CPU	>Simulated attack scenarios like, on-off attack, selective at-tack, bad mouthing etc	>Simulation only > Other Security Principles are not handled.
IoTSAT [45]	Generic [Analysis Tool]	>Assess Resilience on Attack Scenarios	Simulations using Framework developed using >Java API of Z3 SMT solver and AUFLIA logic >Threat Propagation Model	>PC with 3.4 GHz Intel Core i7 processor and 16 GB of RAM. >8:1:4 for Sensor:Controller:Act uator	>Recommendations to increase resiliency >Prevention of Threat Propagation	>Simulation only >Other Security Principles are not handled.
Mobility-First Architecture [48]	Generic	>A mobility centric approach >Key provisioning Protocol	A prototype of the delegation-based key provisioning protocol using wolfSSl and mbedSSL	Linux Machine	>lightweight key provisioning tested for function delegation &ownership transfer	>Talks only about Key provisioning >Other Security Principles are not handled.
SODA [51]	Generic	>Software Defined framework for SDN and NFV	>SODA protocol using C modifying Open vSwitch >mininets >glib hash tables >NFV client in Python	Ubuntu 16.04 (Linux kernel v4.9) and deployed in an Odroid-XU3 board	>Bonet mitigation >network Attack Mitigation >Remote Exploit Mitigation	>IoT Gateway security not handled

They have presented an integral framework which extends the security functionalities defined by the Architectural Reference Model (ARM) from the EU FP7 IoT-A project, focusing on authentication and authorization mechanisms to protect the access to services to be leveraged in smart buildings. It uses XACML (eXtensible Access Control Markup Language) to specify the access policy for service discovery and JSON (JavaScript Object Notation) for service description.

In another work here [40] authors provides a static permission analysis tool for Google Fit-enabled apps. This work is specific to Google Fit Android application and the permissions it requests to provide the services. It was designed to check the grant of over-privileges to third party applications to access the health and fitness related data on Android platform.

The work in [41] is specific to Industrial IoT applications. It proposes a framework to record everyday information of all activities happening at different locations in a Blockchain to ensure secure product shipment, trace workers locations and product documentation. Proposed framework requires two ends, a front end attached to receivers and a back end responsible for internal communication using the Blockchain system. The requests acts as a link between them.

Functionality Specific frameworks are those which provides solutions only for a specific task like, identity management, enforcing privacy, service discovery and so on. Protocol specific frameworks are those which provides solutions for vulnerabilities present in the protocols by design and eliminate the possibilities of security attacks. Publish-Subscribe based IoT services and protocols like MQTT are a few examples under this category.

One of the works done here [42] discusses the requirement for an identity management for publisher and subscriber based cloud based IoT systems. It provides basic functionalities like, registration of sensors and receiver device to the cloud, Identification of hosted services, Authentication/ Login of sensors and receiver device, addition of new device, deletion of existing device and relocation of devices.

Further, here [43] proposes a Model-Driven Security policy enforcement framework, named MDSIoT, for IoT tenant apps deployed in edge servers. This allows execution of policies specified at the model level and then transformed into the code that can be deployed for policy enforcement at run-time. It also supports for the interoperability of IoT tenant apps when deployed in the edge to access IoTaaS services. A proof-of-concept of the proposed gatekeepers based on ThingML, derived from execution policies has been developed.

Another Functionality based work here [44] proposes a trust framework for service discovery in IoT devices. It works in a decentralized manner on top of a structured P2P network based on a Distributed Hash Table (DHT). By utilizing DHT, it proposes a novel way of choosing Reference Holders that prevents the malicious nodes to control these nodes. Protocols designed provide trust aggregation, service provision and feedback aggregation. A threat model in which attacker provides on-off, bad mouthing, ballot stuffing and selective attacks has been simulated. It guarantees a network-wide probabilistic security.

Generic IoT security frameworks are those which can be applied for any IoT application which is built on the reference architecture. A work here [45] presents IoTSAT, a formal framework for Security Analysis of IoT. It formally models the generic behavior of IoT system, based on device configurations, network topologies, user policies and IoT specific attack surface. These models have been formulated using Satisfiability Modulo Theories (SMT). Also, an IoT Threat Propagation model is built to classify IoT threats as interlinked threat vectors where injection of one vector by the attacker can trigger a chain reaction impacting multiple IoT entities. The model is then used to measure system's resilience against potential attacks and identify threat vectors and specific attack techniques, which can be used to achieve higher-level adversary's objectives. Java API of Z3 SMT solver and AUFLIA logic is used to implement IoTSAT. It is also evaluated over realistic IoT networks to show how it can uncover complex attack vectors of IoT systems. It is evaluated on an example scenario of a Building Management System.

Privacy is equally important in designing a secure IoT System. The work here [46] proposes a Privacy-by-Design framework (dry run) for assessing IoT applications and platforms. It lists 30 guidelines including data acquisition,

data sources, data intake, knowledge discovery, data storage, retention period, routing, anonymization of data etc. It classifies the risk into two types namely, Secondary Usage and Unauthorized Access. It also accesses the design for Certification, Standardization and Compliance. Two corporate platforms Eclipse SmartHome and OpenIoT are evaluated against the framework using the color code that the authors propose. Gaps in the privacy can be attacked at the design phase itself. Advantage is that it can be used by non-specialized IT professionals to assess the existing privacy capabilities of IoT middleware.

A generic framework is suggested here in [47], which considers a four layer IoT architecture consisting of Things Layer, Communication Layer, Infrastructure Layer and Data Analysis Layer. It lists the security requirements of each of the layers and proposes a framework to realize the same. It also tabulates the components in each layer and lists the security requirements. IoT Sensor node and Base station in the Things Layer. Network, Wireless Protocol and Tower in the Communication Layer, Cloud and Storage in Infrastructure Layer. Data Analytics in the Data Analysis Layer. It mentions that the security issues are considered by the list provided by the OWASP IoT top ten project which includes, insecure Web/Cloud or Mobile Interface, Insufficient Authentication and Authorization, Insecure Network Services, Lack of Transport Encryption, Privacy Concerns, Insufficient Security Configurability, Insecure Software/Firmware and finally Poor Physical Security. However, the authors mention that they will be developing the IoT system based on the proposed framework in the future and hence no results to discuss.

In [48] an IoT Name Resolution System (IoT-NRS) is proposed as a core component of the middle ware of a Mobility First IoT architecture. It is designed specifically for those applications which has low-end limited capability IoT devices at the things layer. These devices don't support traditional security mechanisms which are heavy weight. Hence, the authors develop a light weight keying protocol that establishes trust between an IoT node and the IoT-NRS. It discusses a Mobility first IoT middle-ware consisting of three layers namely aggregator, local service gateway & Server.

A three-tier name resolution framework of the MobilityFirst-based IoT architecture is proposed providing three services namely, name certificate & resolution service (NCRS), global name resolution service (GNRS) and IoT Name Resolution Service (IoT-NRS). Finally a light weight keying protocol is developed customizing the Choo's three-party key distribution protocol (3PKD) and the SIGMA (SIGn-and-Mac) protocol. A prototype developed with the light weight crypto libraries wolfSSL and mbed SSL is tested on a Linux system with Child, Guardian and Parent setup of a modularized prototype framework design.

In a recent work here [49] eight different Industry IoT Security Frameworks are reviewed considering the following aspects, architecture components, programming languages supported, hardware dependencies, software dependencies, compatible hardware, supported application protocols and under security, authentication mechanisms, access control mechanisms, security in communication, cryptography. Architectures of smart things by Samsung, AWS IoT by Amazon, Calvin from Ericsson, Brillo/Weave by Google, Kura by Eclipse, ARM Mded by ARM, HomeKit by Apple and Azure IoT by Microsoft has been considered for comparison. It discusses many security flaws and lacuna like, insufficient memory for OS, design flaws which expose the users to significant security threat in absence of good practices, dependence on COTS micro-controllers with minimum security support, lack of computing capabilities to run high end encryption algorithms, no option of changing the key after deployment, outdated hardware with outdated encryption algorithm support for long lived nodes, privacy issues with SDKs offered to third party developers and lack of flexibility in the security framework.

In one of the latest work here [50], a new security framework with the following mechanisms are proposed, Robust Authentication, Symmetric Encryption and Light-Weight Cryptography, Secure Authentication, Authorization and Access Control, Intelligent IDS(Intrusion Detection System) and SDN. For a robust authentication, it suggests the use of Bio-metric authentication and Multi-Factor Authentication(MFA). PFUs and hardware obfuscation for access control. It also suggests the use of artificial intelligence, machine learning and deep learning based IDS for adaptability. A linear regression and support vector machine based classification model is suggested for IoT intrusion detection and mitigation model. With all these improvements and suggestions, the authors discuss a new security framework and plan to evaluate it against metrics like, processing response time, resource consumption, attacks mitigation and scalability. In the latest work here [51], just as [46], the focus is on security policy enforcement and security function management. A new Software Defined security framework (SODA) is proposed for the same. The design of SODA consists of the control plane, which manages the network elements and states, provides base security functions sand detects and resolves policy conflicts. Further it contains a function plane, containing pool of computing nodes to perform security functions from IoT devices by employing NFV techniques. The design also consists of a protocol called SODA for communication between function plane and data plane. The protocol design comprises of handshake process, policy installation and information delivery. Finally, the core module of the SODA architecture consists of a Policy manager, Session manager and NFV manager. It is implemented and tested on top of an Ubuntu and Odroid-XU3 board using. Control plane is developed using C libraries, Open vSwitch a software switch and NFV client in Python. On the test-bed setup, they test it for user defined access control, policy conflict detection and resolution.

V. CONCLUSION

This paper has surveyed all the available IoT security frameworks and results with a comparison of each based on the following metrics, a) Type b) focus area c) Implementation d) Test-Bed Setup e) results f) lacuna/limitations reported. The comparison of few of the frameworks surveyed in this work are also tabulated. It has been concluded that various aspects of IoT security keeps changing and a need for a more adaptable IoT security framework is also made evident. Among the frameworks discussed above, majority are implemented and tested but few are just discussed conceptually.

However, the application of blockchain [19], machine learning concepts like, linear regression and support vector machine to implement intelligent intrusion detection

system [50] at edge is a commendable contribution. Work in this direction will help in creating a secure IoT application.

Further, this research work should proceed on designing a new framework which is, a) adaptable and application agnostic b) supports SDN and NFV c) continuously refresh/change the keys for robust authentication d) role based authorization and access control e) usage of AI/ML and DL mechanisms on edge devices for intrusion detection f) Usage of micro services for authentication and other possible improvements. It should also be tested on multiple real world scenarios and analyzed.

REFERENCES

[1] Mikhail Gloukhovtsev "IoT Security: Challenges, Solutions & Future Prospectus", DELL, Knowledge Sharing Article, 2018

[2] V. Hassija et al. "Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", IEEE Access, Volume 7, pp. 82721-82743, 2019

[3] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. pp. 1282–1285, 2012

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] 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 & Tutorials, vol. 17, no. 4. pp. 2347–2376, 2015.

[6] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: A study," Int. J. Comput. Sci. Eng. Surv., vol. 2, no. 3, pp. 94–105, 2011.

[7] Munir A, Kansakar P, Khan SU, "IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things", IEEE Consumer Electronics Magazine. Jun 14;6(3):74-82, 2017

[8] Kapsalis A, Kasnesis P, Venieris IS, Kaklamani DI, Patrikakis CZ, "A cooperative fog approach for effective workload balancing", IEEE Cloud Computing. Apr 26;4(2):36-45, 2017

[9] Fan, Q. and Ansari, N., "Application aware workload allocation for edge computing-based IoT", IEEE Internet of Things Journal, 5(3), pp.2146-2153, 2018

[10] Yogi MK, Chandrasekhar K, Kumar GV. "Mist Computing: Principles, Trends and Future Direction", arXiv preprint arXiv:1709.06927, Aug 6, 2017

[11] Mahmoud Parto et al, "A Novel Three-Layer IoT Architecture for Shared, Private, Scalable, and Real-time Machine Learning from Ubiquitous Cyber -Physical Systems", Science Direct, Procedia Manufacturing 48, pp. 959–967, 2020

[12] Lidiane Santos, Eduardo Silva, Thais Batista, Everton Cavalcante, Jair Leite and Flavio Oquendo, "An Architectural Style for Internet of Things Systems", In The 35th ACM/SIGAPP Symposium on Applied Computing (SAC'20), March 30-April 3, 2020

[13] Anthony Sabella, Rik Irons-Mclean, Marcelo Yannuzzi, "Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT", Cisco Press, ISBN: 9780134756936, 2018

[14] Yuhong Li ; Xiang Su ; Jukka Riekki ; Theo Kanter ; Rahim Rahmani, "A SDN-based architecture for horizontal Internet of Things services", 2016 IEEE International Conference on Communications (ICC), 2016

[15] Nikos Bizanis ; Fernando A. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey", IEEE Access (Volume: 4) 09 September 2016

[16] Harshith Arun Kumar et al., "Comparison Of IoT Architectures Using A Smart City Benchmark", Science Direct, Procedia Computer Science, 171, 1507–1516, 2020

[17] Maha Saadeh, Azzam Sleit, Khair Eddin Sabri, Wesam Almobaideen, "Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities", Journal of Network and Computer Applications 121, Elsevier, 2018

[18] Randa M. Abdelmoneem, Abderrahim Benslimane, Eman Shaaban, "Mobility-aware task scheduling in cloud-Fog IoT-based healthcare architectures", Computer Networks 179 , 107348, Elsevier, 2020

[19] Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT", Journal of Network and Computer Applications 149, 102481, Elsevier, 2020

[20] Arsalan Mosenia , Niraj K. Jha, "A Comprehensive Study of Security of Internet-of-Things", IEEE Transactions on Emerging Topics in Computing, Volume 5, No.4, pp. 586-602, 2017

[21] Mardiana binti Mohamad Noor, Wan Haslina Hassan, "Current research on Internet of Things (IoT) security: A survey", Computer Networks 148, 283–294, Elsevier, 2019

[22] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636-1675, 2019

[23] "Threat Landscape Trends – Q1 2020", 9th June 2020, Accessed on: 5th July 2020, [Online] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020

[24] "FAQ about Cyber Attack on VTech Learning Lodge" January 9, 2018, Accessed on: 5th July 2020, [Online] https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/

[25] Nick Statt, "How an army of vulnerable gadgets took down the web today", Oct 21, 2016, Accessed on: 5th July 2020, [Online] https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

[26] "KerbsonSecurity", Accessed on 5th July 2020, [Online] https://krebsonsecurity.com/

[27] Selena Larson, "FDA confirms that St. Jude's cardiac devices can be hacked", January 9th 2017, Accessed on: 5th July 2020, [Online] https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/

[28] Gary Davis, "Casino's High-Roller Database Compromised by a Single IoT Thermometer", 17th April 2018, Accessed on 5th July 2020, [Online] https://www.mcafee.com/blogs/consumer/consumer-threat-notices/casinos-high-roller-database-iot-thermometer/

[29] "Silex Malware Bricks IoT Devices with Weak Passwords", 27th june 2019, Accessed on: 5th July 2020, [Online] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-silex-malware-bricks-iot-devices-with-weak-passwords

[30] Lindsey O'Donnell, "IoT Insecurity: When Your Vacuum Turns on You", 27th Feb 2020, Accessed on: 5th July 2020, [Online] https://threatpost.com/vacuum-cleaners-baby-monitors-and-other-vulnerable-iot-devices/153294/

[31] Sean Hollister, "Your Philips Hue light bulbs can still be hacked — and until recently, compromise your network", 5th Feb 2020, Accessed on: 5th July 2020, [Online] https://www.theverge.com/2020/2/5/21123491/philips-hue-bulb-hack-hub-firmware-patch-update

[32] S. Pallavi and V. A. Narayanan, "An Overview of Practical Attacks on BLE Based IOT Devices and Their Security," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 694-698, doi: 10.1109/ICACCS.2019.8728448.

[33] S. Khanji, F. Iqbal and P. Hung, "ZigBee Security Vulnerabilities: Exploration and Evaluating," 2019 10th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2019, pp. 52-57, doi: 10.1109/IACS.2019.8809115.

[34] O. Westerlund and R. Asif, "Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things," 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS), Muscat, Oman, 2019, pp. 1-10, doi: 10.1109/UVS.2019.8658279.

[35] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes, "Exploring the Security Vulnerabilities of LoRa," 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, 2017, pp. 1-6, doi: 10.1109/CYBConf.2017.7985777.

[36] R. Sahay, G. Geethakumari and K. Modugu, "Attack graph — Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 308-313, doi: 10.1109/WF-IoT.2018.8355171.

[37] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-7, doi: 10.1109/ICBDSC.2016.7460363.

[38] S. Andy, B. Rahardjo and B. Hanindhito, "Attack scenarios and security analysis of MQTT communication protocol in IoT system," 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, 2017, pp. 1-6, doi: 10.1109/EECSI.2017.8239179.

[39] José L. Hernández-Ramos, M. Victoria Moreno, Jorge Bernal Bernabé, Dan García Carrillo, Antonio F. Skarmeta,"SAFIR: Secure access framework for IoT -enabled services on smart buildings, Journal of Computer and System Sciences",Volume 81, Issue 8, Pages 1452-1463, 2015

[40] Nobakht, Mehdi & Sui, Yulei & Seneviratne, Aruna & Hu, Wen, "PGFit: Static permission analysis of health and fitness apps in IoT programming frameworks", Journal of Network and Computer Applications. 152. 102509, 2019

[41] Rathee, Geetanjali & Sharma, Ashutosh & Kumar, Rajiv & Iqbal, Razi, "A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology", Ad Hoc Networks 94 (2019) 101933, Elsevier, 2019

[43] Susmita Horrow, Anjali Sardana, "Identity Management Framework for Cloud Based Internet of Things", SecurIT'12, pp. 200-203, ACM, 2012

[43] Phu H. Nguyen, Phu H. Phung, Hong-Linh Truong, "A Security Policy Enforcement Framework for Controlling IoT Tenant Applications in the Edge", IOT '18, ACM, DOI: https://doi.org/10.1145/3277593.3277602, 2018

[44] Kübra Kalkan, Kasper Rasmussen, "bTruSD: Trust framework for service discovery among IoT devices", Computer Networks 178 (2020) 107318, Elsevier, 2020

[45] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer and M. A. Rahman, "IoTSAT: A formal framework for security analysis of the internet of things (IoT)," 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 180-188, doi: 10.1109/CNS.2016.7860484.

[46] Charith Perera, Ciaran McCormick, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms", 6th International Conference on the Internet of Things (IoT'16), ACM, doi: http://dx.doi.org/10.1145/2991561.2991566 , 2016

[47] Abdul Fuad Abdul Rahman, Maslina Daud, Madihah Zulfa Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework", ICC '16, ACM, doi: http://dx.doi.org/10.1145/2896387.2906198

[48] Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture", Future Internet 2017, 9, 27; doi:10.3390/fi9030027

[49] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, "Internet of Things: A survey on the security of IoT frameworks" , Journal of Information Security and Applications 38 (2018) 8–27, Elsevier, 2018

[50] Aliya Tabassum, Wadha Lebda, "Security Framework for IoT Devices against Cyber-Attacks", International Conference on Internet of Things (CIoT 2019), arXiv:1912.01712

[51] Yeonkeun Kim, Jaehyun Nam, Taejune Park, Sandra Scott-Hayward, Seungwon Shin, "SODA : A software-defined security framework for IoT environments", Computer Networks 163 (2019) 106889, Elsevier, 2019

[52] Melissa Michael, "Attack Landscape H1 2019: IoT, SMB traffic abound", 12th September 2019, Accessed on 7th July 2020, [Online] https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/