An EXPERIMENTAL ANALYSIS OF SECURITY VULNERABILITIES IN INDUSTRIAL INTERNET OF THINGS SERVICES

Tarun Dhar Diwan
Chhattisgarh Swami Vivekanand, Technical, University
Bhilai, Chhattisgarh, India.
tarunctech@gmail.com

Dr. Siddartha Choubey
Shri Shankaracharya Technical Campus,
Bhilai, Chhattisgarh, India.
sidd25876@gmail.com

Dr. H.S. Hota
Atal Bihari Vajpayee University
Bhilai, Chhattisgarh, India.
proffhota@gmail.com

Abstract:
Information exchange by device to device was mainly active while in beginning of the IoT. The approach has increasingly expanded to incorporate human experiences as well, leading to an age of Internet-of-Everything. A large proportion among applications, along with smart cities, Overcrowding and waste disposal, overall well-being, defense, sales, operations, emergency services, Medical treatment and factory control, are empowered by IoT technology. IoT is a technology on a grand scale connect to something, anything, at any moment, location, platform support, as well as other node. This one has a major impact over the whole block chain. Heterogeneous network connectivity-enabled organizations, intelligent objects and applications, networks as well as program that are built as a clever, universal system of smart devices. In several areas, The Internet of Things (IoT) is in operation, and it binds to complicated systems, communicate through extreme atmospheres, and distributed upon several unrestrained frameworks, so they face numerous protections problems as well as difficulties Since the Internet of Things represents a possible forum to incorporate any kind of network and complicated structure, flaws inherent in the individual structures accessible across the embedded network may be encountered. This paper discusses the security concerns of individual IoT interlinked systems and their effect on the interconnected IoT device.

I. Introduction

Our planet today contains a tremendous number of devices and mobile equipment that constantly track, gather, consolidate, and process a convincing amount of our personal data [1]. Our area, contact list, surfing activities, and fitness and health records might include such details [2]. Computer devices mainly motivate the detecting, collection and dissemination of certain intense private information through personal computers: When systems become intelligent, it may be able to properly respond to our wants, desires, as well as emotions and remedy the situation (e.g., a residential security system can react to a fire or break-in). Unfavorably, this simplicity leads to the problem of protection & unauthorized, malicious agent, confidential, personalized details will result in substantial harm to our assets, public image, as well as personal protection [3]. This system also carries properties in addition to our private info added during manufacturing supply chain by their suppliers at different times. These have modes that Fuse, firmware, and debugging are also included. Access to such properties without authorization would result in the destruction of millions of dollars in patented copyrights and the potentially harmful misuse of assets [4]. These vulnerability flaws can be disastrous with the ubiquitous implementation of these appliances. The point of creating such potentially disastrous flaws in electronic systems is not simply academic. Unfortunately, that can happen all too quickly in reality. There have been several demos that by using the programming interface, attackers can quickly insert direct injection of malicious

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

programs into a wearable interface and then gain confidential user data. Targets towards pharmaceutical devices that are implanted, like implantable cardioverter defibrillators [5], have been found to severely endanger patient protection. A growing trend is also seen by attacks on business and urban infrastructure. increasing number computing sensors and integrated instruments are found in several upscale vehicles in field of automotive embedded systems. Because of the lack of security safeguards at those systems, like the electronic control unit attack, the intruder will take control of the vehicle [6]. This will pose a significant safety threat to the driver. Attacks on urban infrastructure, such as attacks on transportation and logistics, will impact the social order [7]. We consider the continuum of IoT security problems, methods, and experience in this article. In certain ways, IoT protection is special and faces numerous problems distinct from those in other electronic devices' security assurance, such as desktops, notebooks, servers, or even personal devices [8]. on every layer of the IoT, we routinely examine security risks and privacy problems [9]. Attacks will take place on each layer, and we need to secure the whole framework of the IoT, not just the basic technologies. Various device scenarios are based on taxonomy of IoT protection and vulnerabilities. This offers an empirical framework for numerous IoT technologies to be covered. Treaties against Internet of Things (IoT) design are defined, and a variety of attack scenarios are elaborated. we discuss those IoT security problems [10]. the viewpoint of IoT security specifications, we discuss the concept protection system and security mechanism.

II. Types of IoT Networks

Networks are divided into categories based on the distance range they provide.

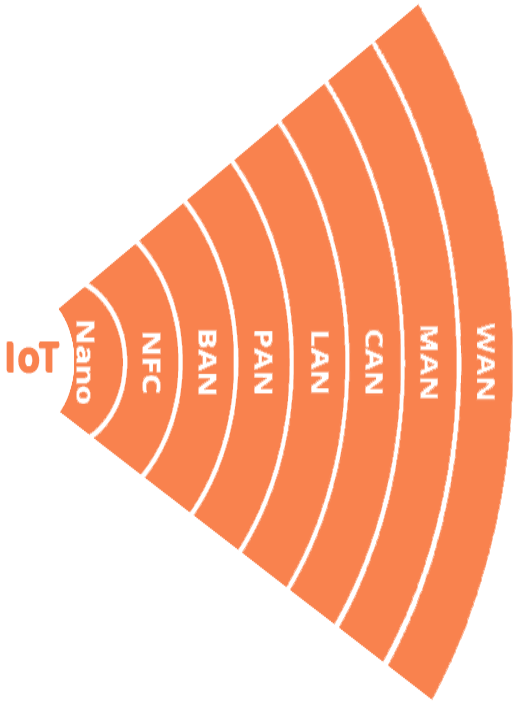

Figure 1: Types of IoT Network

a) **WAN (Wide Area Network):** A network that stretches across a wide geographical region and puts together numerous smaller networks, including LANs and MANs.

b) **MAN (Metropolitan Area Network):** A large network operated by microwave transmission technologies over a certain metropolitan are a [11].

c) **CAN (Campus/Corporate Area Network)** A network that unites smaller networks of local communities within a restricted geographical region (enterprise, university).

d) **LAN (Local Area Network)** A network that covers one building's area.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

e) **PAN (Personal Area Network)** a net to link up devices within a radius of roughly one or a couple of rooms.

f) **BAN (Body Area Network)** a network to connect wearable computing devices that can be worn either fixed on the body, or near the body in different positions, or embedded inside the body (implants).

g) **NFC (Near-Field Communication)** a low-speed network to connect electronic devices at a distance within 4 cm from each other. Possible applications are contactless payment systems, identity documents and keycards [12].

h) **A Nano Network** a set of small devices (sized a few micrometers at most) that perform very simple tasks such as sensing, computing, storing, and actuation. Such systems are applied in biometrical, military and other nanotechnologies [13].

III. Classification of IoT Security Attacks.

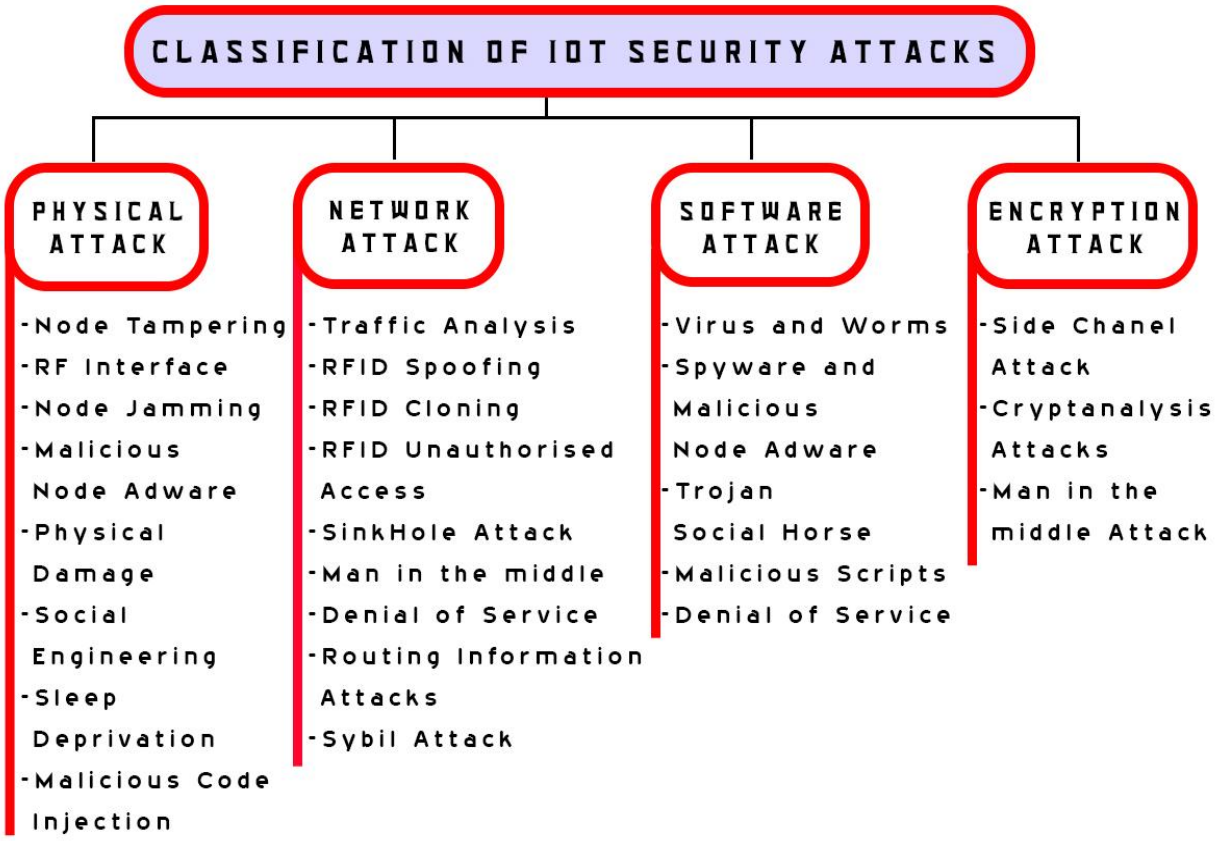

Figure 2: Classification of IoT Security Attacks

A. Physical Attacks

It is focused on the system's hardware components.

1) Node Tampering: Physically modification the vulnerable node in this assault intruder and may access confidential data such as encryption key.

2) RF Interference on RFIDs: By transmitting noise signals over radio frequency signals, the intruder conducts a Denial - of - service. For

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

RFID communication, certain signals are used [14].

3) Node Jamming in WSNs: The intruder will interfere with wireless communication by using a jammer. This induces service assault denial.

4) Malicious Node Injection: In this attack, a new malicious node is physically inserted between two or more nodes by the attacker. It then alters the data to transfer the erroneous data to other nodes [15].

5) Physical damage: The hacker physically destroys IoT device components which results in a Denial-of-Service attack [16].

6) Social Engineering: The perpetrator physically communicates with members of an IoT device and manipulates them. To fulfill his aims, the perpetrator obtains classified information [17].

7) Sleep Deprivation Attack: The attacker's intention is to use extra power to temporarily close nodes [18].

8) Insertion of malicious code: The adversary physically inserts a malicious code into the IoT device node. The intruder is able to get total control of the IoT system [19].

B. Encryption Attacks

Such attacks rely upon breaking encryption by extracting its secret keys.

1) Side-channel Attacks: The intruder uses information from the side channel that is emitted by system encryption. It is not the plaintext or the cipher text, it contains power information, the time taken to perform the operation, the frequency of faults, etc. This data is used by the intruder to detect the secret keys [20].
There are various kinds of side-channel attacks, such as timing attacks, Simple and Differential Power Analysis, and Attacks for Differential Fault Analysis.

2) Timing Attack: Timing attacks are based on the time needed for operations to be carried out. This includes information about the hidden keys. An attacker can obtain fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems by using this knowledge [21].

3) Cryptanalysis of a Simple Modular Exponentiation: Diffie-Hellman and RSA operations involve calculation of $R = y \bmod n$, where n is public and y can be obtained by a listener [22].

C) Cryptanalysis Attacks: During this attack, by using either plaintext or cipher text, the adversary obtains the encryption key. There are distinct types of cryptanalysis attacks depending on the methods used [23].

1) Cipher text Attack only: This helps the attacker to view the cipher text and to decide the necessary plain text [24].

2) Known Plaintext Attack: In this form, for certain parts of the cipher text, the attacker knows the plaintext. The goal is to decrypt the remaining part of the cipher text that uses this data [25].

3) Plaintext Attack Chosen: The attacker will pick which plaintext is encrypted and find the key for encryption.

4) Chosen Cipher text Attack: The attacker finds the encryption key by using the plain text of the chosen cipher text [25].

D) Man in the Middle Attacks: The attacker intercepts the conversation and acquires the secret key when two people exchange the Secret key [26].

E. Network Attacks

Such attempts are aimed at the IoT device's infrastructure.

1) **Traffic Analysis Attacks:** To gain network information, the attacker intercepts and analyses replies.

2) **RFID Spoofing:** RFID signals are spoofed by an adversary. The information which is

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

transmitted from an RFID tag is then captured. Spoofing attacks send misleading data that seems to be right and that is approved by the system [27].

3) **RFID Cloning:** During this attack, the opponent copies data to another RFID tag from a pre-existing RFID tag. It does not copy the RFID tag's original ID. The attacker is able to insert incorrect data or monitor the passage of data through the cloned node [28].

4) **RFID Unauthorized Access:** When the RFID systems do not have proper authentication, then the opponent will monitor, change or delete information on nodes [29].

6) **Man in the Middle Attacks:** The intruder intercepts contact between both the pair of nodes over the internet. By eavesdropping, they collect confidential data [30].

7) **Denial of Service:** An intruder loads the channel with heavy traffic so that its intended users do not have access to the services [31].

8) Routing Information Attacks: During this attack, by spoofing, altering or sending routing information, the attacker can render the network complex. It leads in packets being permitted or dropped, incorrect data being forwarded or the network partitioned [32].

9) **Sybil Attack**: Suspicious nodes which takes the identities of several nodes and behaves like them in this attack. For example, in the Wireless Sensor Network, the single node voting system may vote several times [33].

F. Software Attacks

For stealing information, refuse facilities, and so on, the intruder employs viruses, parasites, ransomware, and bloatware.

1) Phishing Attacks: The intruder acquires private data such as user-name, passwords by e-mail spoofing and by using fake sites [34].

2) **Virus, Worms, Trojan Horse, Spyware and Aware:** By using malicious code, an adversary will harm the device. Via email attachments, these codes are transmitted by downloading files from the Internet. Without any human action, the worm has the capacity to reproduce itself. To detect the virus, we can use worm detectors, anti-viruses, firewalls, intrusion detection systems [25].

3) **Malicious Scripts:** An attacker can gain access to the system by injecting a malicious script.

4) **Denial of Service:** By refusing services, the attacker excludes users from the application layer.

Companies in the technological fields, entertainment, media, as well as t-communications, take a common approach. According to the same survey, percent of them included cyber security also as deciding factor in business decisions [26].

Table 1: Cyber security Survey

	2012	2014	2016	2018	2020
1	Insufficient financial capital	Insufficient financial capital	Insufficient financial capital	Insufficient financial capital	Insufficient Cyber security budget

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

2	Risks are getting more complex	Risks are getting more complex	Risks are getting more complex	Specialists are not always available	Insufficient Cybersecurity personnel
3	Security Specialists are not always available	Specialists are not always available	Specialists are not always available	Risks are getting more complex and Methodologies are not well reported.	Risks are getting more complex

Source: NASSCIO Cyber security studies.

IV. Analysis of IoT Security, Threats, Attacks and Possible Solutions.

The IoT faces different forms of threats, including aggressive attacks and passive attacks, which can effectively interrupt the features and eliminate the advantages of its services [27]. An attacker only detects the node or can steal the information in a passive attack, but it never strikes physically [28]. the active attacks physically interrupt the effectiveness. Such active threats are split into two additional categories: internal attacks and external attacks. This insecure attack will stop the devices from communicating smartly. Therefore, to protect computers from destructive attacks, security restrictions must be enforced [29].

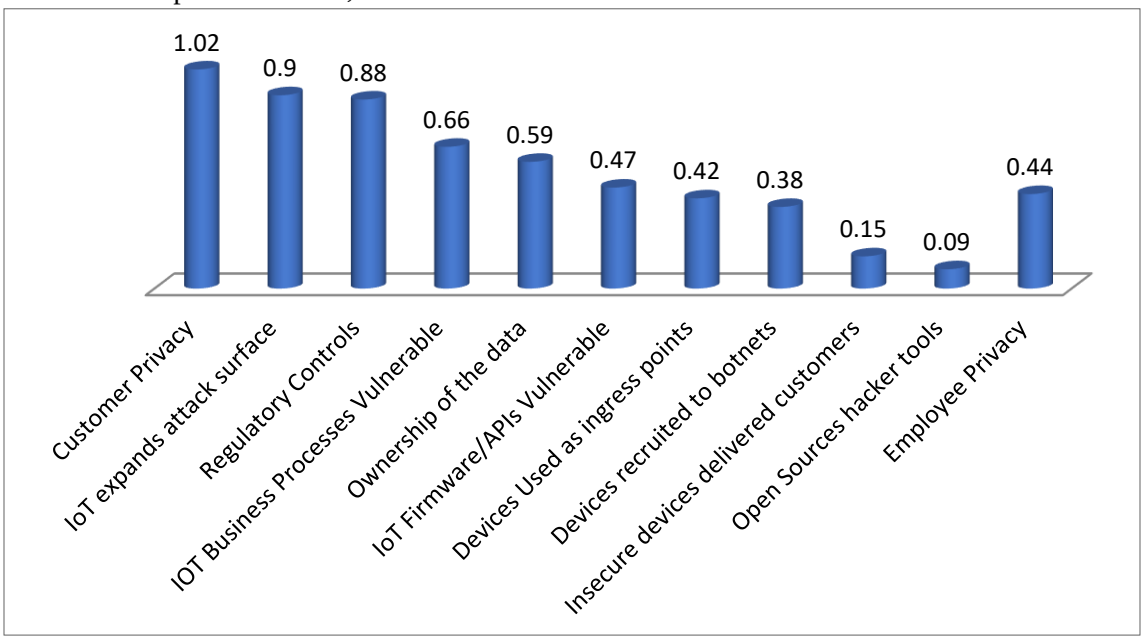

Figure 3: IoT Security Concerns

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

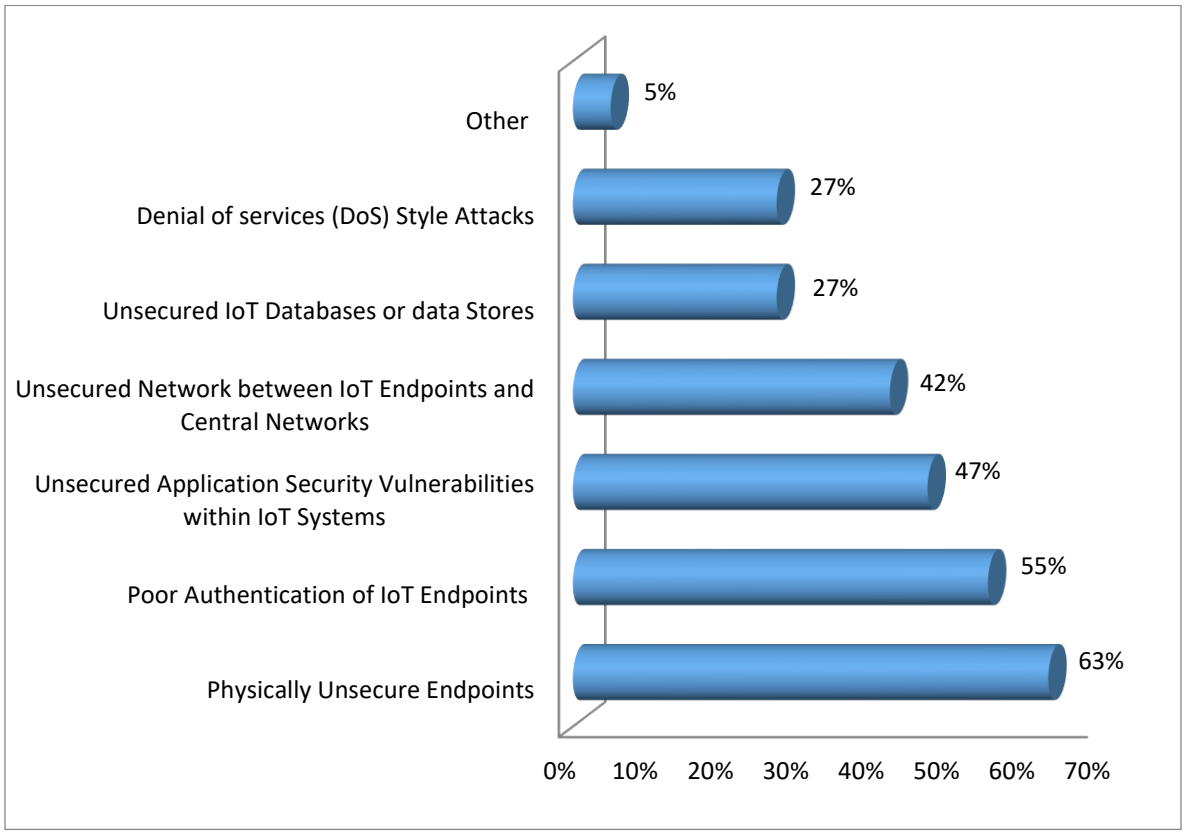

Figure 4: Security Vulnerabilities in web apps

As per studies, website security breaches are still a major issue, with more than a third of internet-dependent web applications classified as high danger.

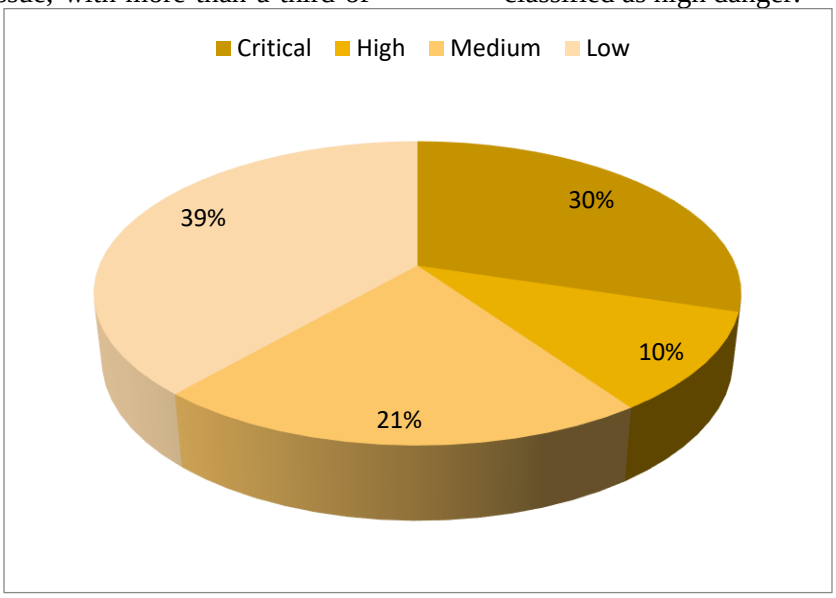

Figure 5: Vulnerabilities in Internet Application

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

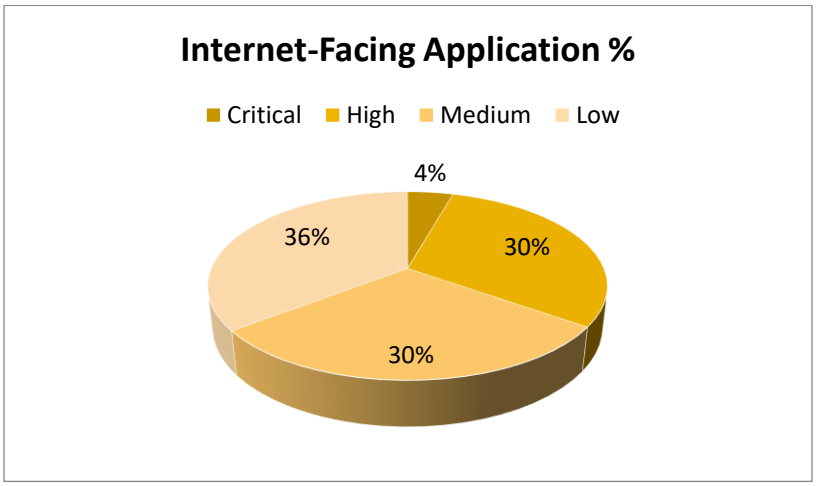

Figure 6: Vulnerabilities in Internet-Facing Application

Source: Cyber security report 2020 by Deloitte-NASCIO

What's more, the dilemma is so severe that even nations are focusing on this part. In 2020, 60 percent of states will review the code and carry out program protection checks. This is an improvement of 6 per cent from 2019[30].

(A) Many by bug bounty schemes, are trying to find and fix vulnerabilities:

- In 2019, Google paid out 2.5 million bug bounties, for a total of 21 million dollar from 2010.
- In 12 months, Microsoft charged almost $14 million worth of bug bounties [31].
- Facebook already has a bounty scheme and in 2020 it will grant about $2 million in just under 10 months. To date, the highest reward has been $80,000[32].
- Vulnerability with a significant or pivotal danger accounted for 40% among all vulnerability. Vulnerability that was moderate at threat accounted for 21.05 percent among all vulnerability. [33].

(B) The number of IoT attacks is on the rise

- Whereas if number of IoT devices keeps going to grow at an exponential rate, so will the corresponding privacy concerns. The statistics speak for themselves[34]. According to estimates, the internet penetration Rate will increase from 31 billion in 2020 to 35 billion in 2021 and 75 billion in 2025 [35].

(C) Protection Today's The 2020 IoT Rundown

- The number of cyber-attacks on IoT users rose by 300 percent in the first half of 2019. (F-Landscape of Stable Attack H1 2019) [36].
- It accounted for 2.9 billion activities which marked the first time that figures approached one billion [37].

(D) F-Secure Attack Landscape Report 2019

- 69% of companies have networks that consist of more IoT gadgets than servers [38].
- 84% of security practitioners claim computers are less vulnerable than IoT machines.
- Threat events affecting IoT products have affected 67% of companies [39].
- Just about 21% of security professionals agree that their existing security measures are appropriate [40].
- With 39 percent calling it a top priority, stability is a key concern for IoT developers [41].

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Compared with 2017, the total number of IoT attacks remained strong in 2018 and stable. The most compromised computers were routers and wired cameras, accounting for 75% and 15% of the attacks, adequately [42].

(E)Vulnerability Study on Internet Protection by Symantec

- Communication protection (43%) and data encryption are the most frequently used techniques in IoT security (41 percent) [43].

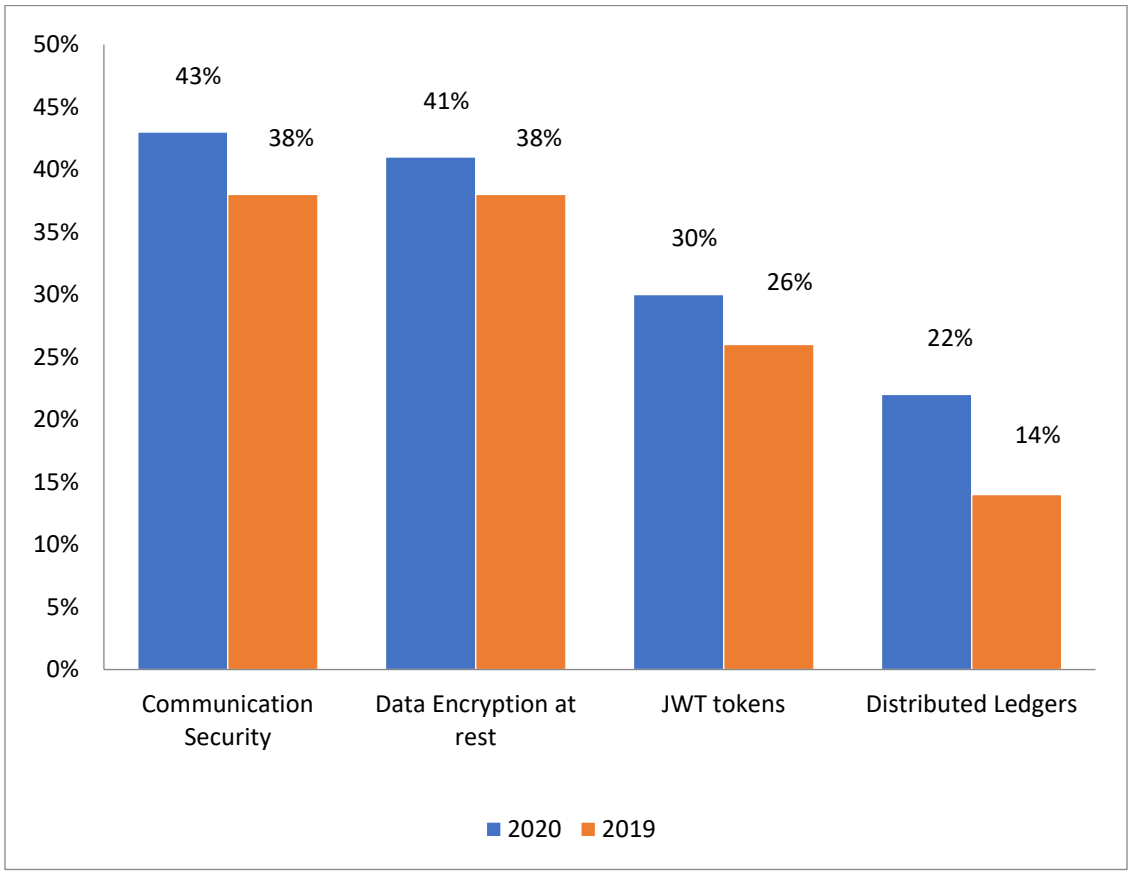

Figure 7: Top Security Technology

(F) IoT Developer Survey Key Findings

- Until 2022, IoT security expenditure is projected to expand at an annual compound growth rate of 44%, reaching nearly $4.4 billion.
- [43].
- Malware was the cause of the majority of IoT security attacks between 2015 and 2017

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

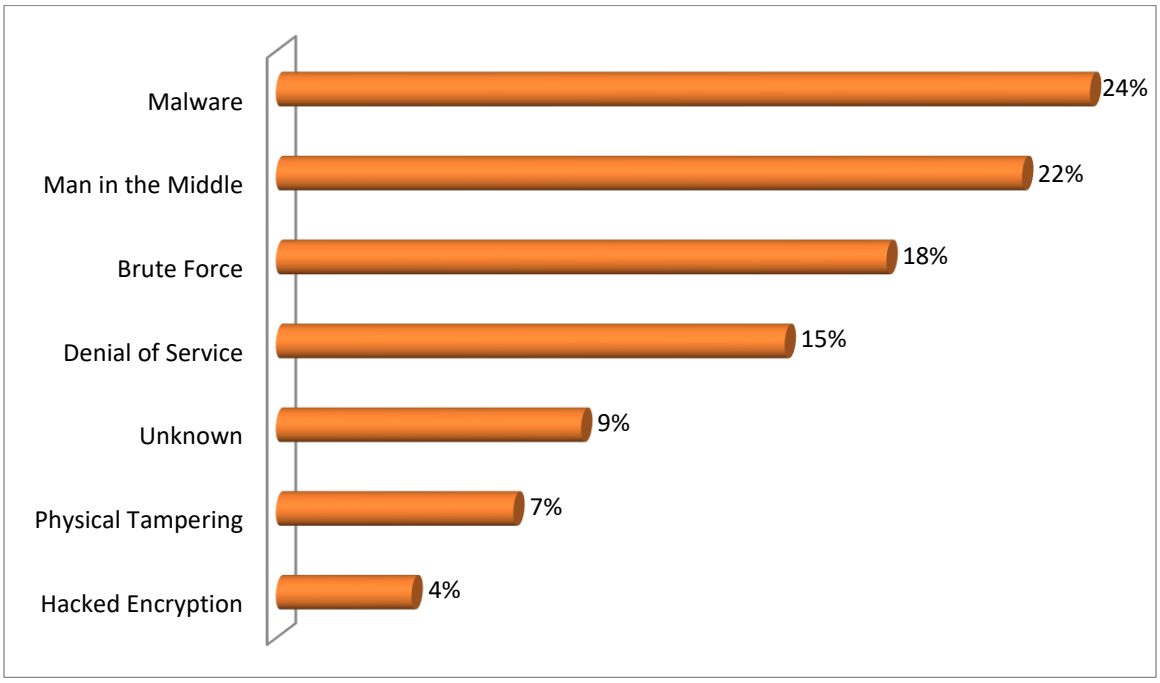

Figure 8: IoT Security Market Report 2017-2022

As we've seen, the core attack strategy is default passwords, so the key IoT protection problems Identity verification (32%) is the most pressing question, guided by access control (15%) and encryption techniques 14 percent [44]. (IoT Security Market Report 2017-2022).

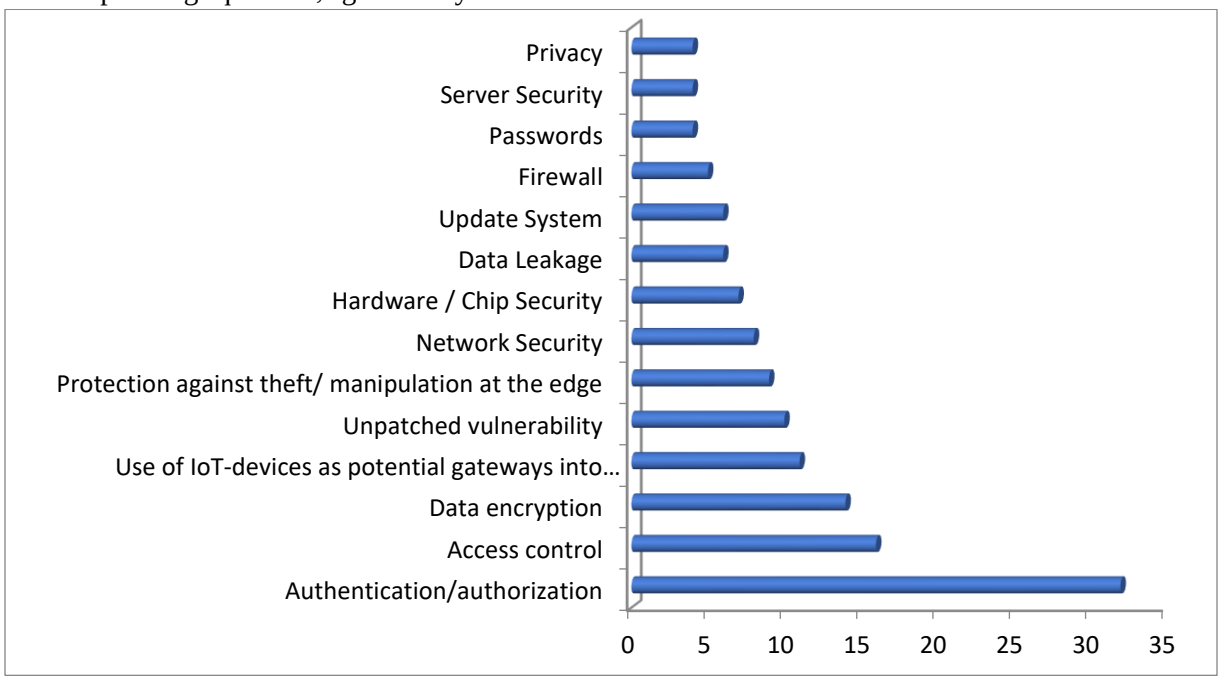

Figure 9: Improvements in IoT security

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

(G) IoT Security Market Report 2017-2022

- 57% of IoT systems could be vulnerable to attack. (The Linked Enterprise's Palo Alto Networks: IoT Security Research 2020) [45].
- Just 4% of developed people think their IoT protection policies have no room for change. 17% say there is a need for a complete redesign [46]. (The Linked Enterprise's Palo Alto Networks: IoT Security Research 2020) [47].
- To boost IoT system security, only around one in five IT decision-makers use micro-segmentation. (The Wired Company in Palo Alto Networks: IoT Security Study 2020) [48].

(H) Social media scams and attacks spread like wildfire

Social networking sites have been a honey mine for cybercriminals and fraudsters, with billions of consumers and daily usage skyrocketing [49]. Social network habits appear to be shifting, but actions do not follow suit, leaving malicious actors with plenty of resources around the globe to steal data and defraud people [50].

- For a whopping 849 million leaked documents in 2019, Facebook leaks were liable. Comparatist.
- When it comes to protecting their entries, 96 percent of Baby Boomers, 94 percent of Generation Xers, 93 percent of Generation Z, and 92 percent of Teenagers fear social networks [51].

A vast majority (94 percent) of all users posting personal details on social networks and 95 percent of client surveyed feel a general sense of mistrust towards social media networks [52]. They would rather forgo using social platforms than search engines if offered the option of "choosing the lesser evil" [53].

(I) Web of Profit: Channels for social media and the cybercrime economy

- 500 social media communities committed to fraud were identified by RSA, with a total of 220,000 users. Among all, 60 percent were on Facebook [54].
- WhatsApp is a common contact medium for fraud, although Twitter is not popular.
- About 15,000 stolen credit cards promoted on different social media networks were noticed by RSA during its analysis [55].
- At least 20 percent of social media infections originate from social media network add-ons or plugins [56].
- Phishing on social media is growing, with social networks responsible for 8% of attacks [57].

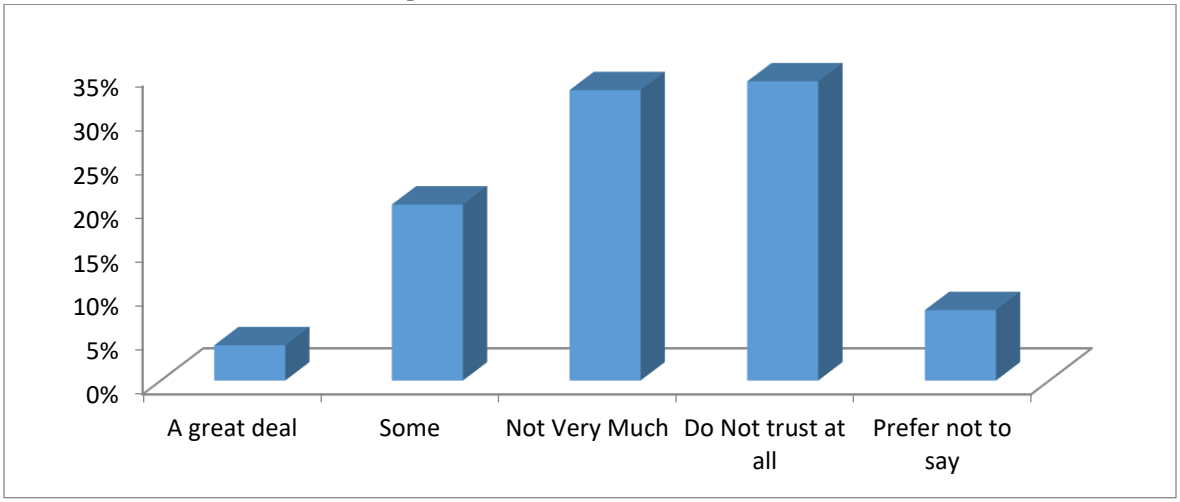

Figure 10: Channels for social media and the cyber - crime economy

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

(J) Cyber security spending trends

Nowadays, nearly everyone is victim of cyber threats. Some firms (about a third) detect threats on a weekly basis and organizations surveyed (93 percent) agree that in the prior 12 months they have suffered a cyber threat [58]. Malicious hackers often have a form: they choose mid-size businesses with 5,000-9,999 workers because they are the most affected by active cyber-attacks [59].

- In 2020, 62% of companies are preparing to invest more on cyber defense.
- 53% of companies in 2018 raised their spending for cyber security [60].
- 15% of organizations have a sizeable IT defense budget of over $10 million, while 37% invest less than $200,000[61].
- 44 percent of 9,500 administrators in 122 countries polled by PWC say they do not have an overall plan for information security [62].
- The dilemma goes broader than that: 48 percent of these 9,500 executives reported that they do NOT have a safety awareness training program for their workers [63].
- In order to help them deal with future threats and compromises, 54 percent of them still lack an incident management process [64].

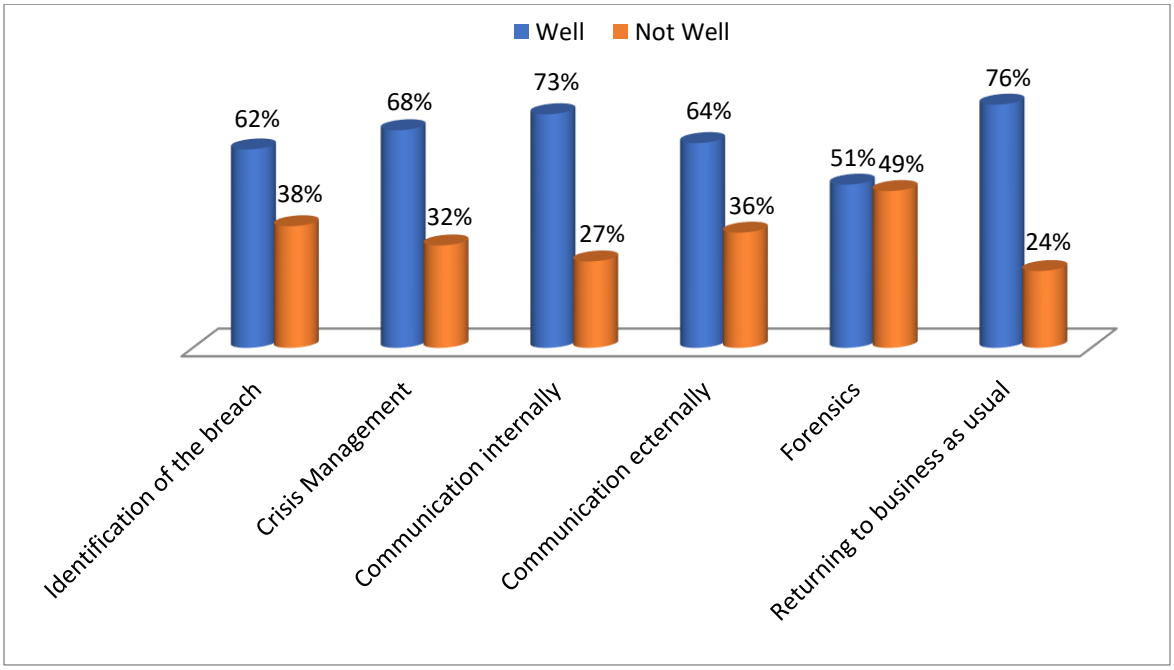

Figure 11: Priorities for improvement when a breach occurs: how organizations perform

(K) Global Information Security Survey.

- For an average of 146 days before detection, an attacker resides within a network. (As from Microsoft) [65].
- 86% of managers believe that "taking business resilience towards the next level requires an impressive new Internet vision [66]."
- On average, 13% of the overall IT budget is taken up by IT security.
- 66% of executives surveyed identify security spending with income from each business line.
- Over 75 percent of their security event data can be processed by only 1 in 10 companies [67].

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

- About 30 percent of businesses that have experienced attacks have not been able to identify the motive [68].
- 41% of business leaders admit costs "at least twice the amount lost to cybercrime on investigations and related interventions [69].
- Only 6 percent of businesses in financial services are truly happy with their cyber security program outcomes [70].

As a whole, 92% of organizations in key areas are concerned about their information security functions. A key problem is resources: 30 percent of companies are struggling with shortages of skills, while 25 percent cite budget constraints [71].

(L) Global Information Security Survey 2018-2019.

Some of the missing puzzle pieces include:

- Better cloud security, as 53% of organizations host at least 50% of their cloud infrastructure[72].
- Upgrading to newer software; 50% of local authorities in the UK, for example, rely on unsupported server software [73].
- Lagging security awareness training: In the last 12 months, only 20 percent of companies have sent any employees to internal or external cyber security training [74].
- Only 27% of UK companies have a formal cyber security policy or policy in place [75].
- Restrictions on human resources: over 50 percent of companies are "re-training current IT employees to address cloud security issues"[76].

(M) Cyber security figures, businesses are trying to progress in a number of ways:

- 85% of businesses are interested in managing pass codes with new authentication forms [77]."53 percent use machine learning for purposes of cyber security".
- 86% of companies have looked into the idea about using machine learning and artificial intelligence implementations [78].
- 51% of organizations surveyed are now investing more in cyber analytics [79].

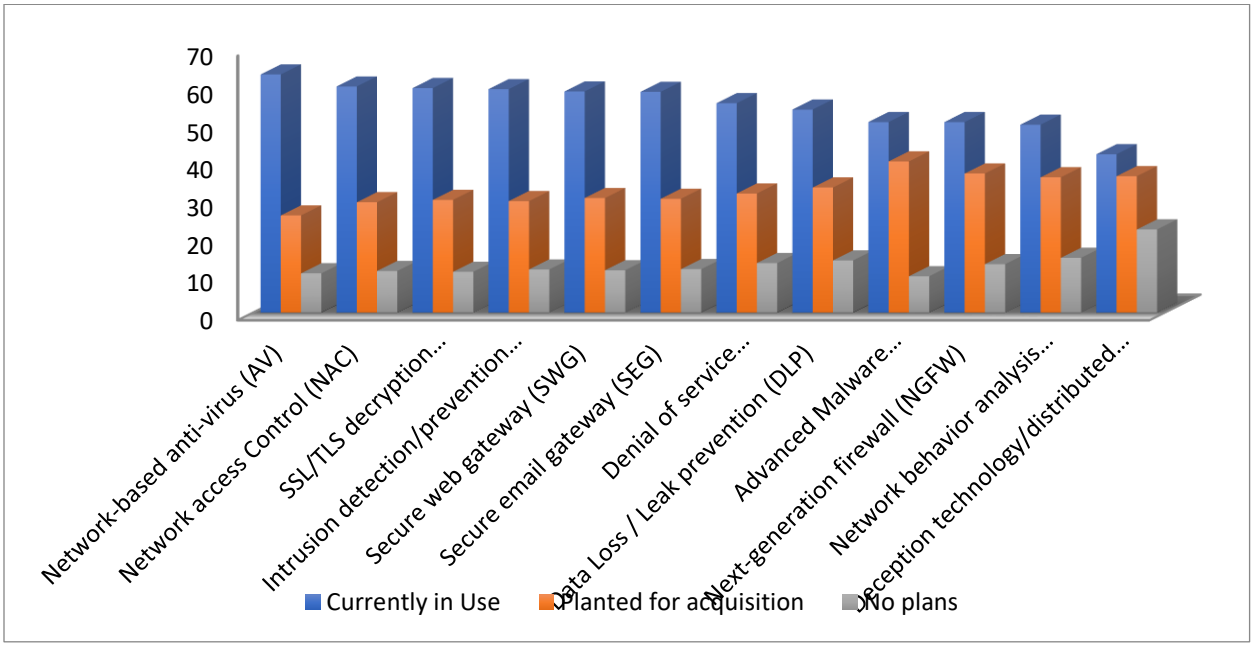

Figure 12: Cyber threat Defense Report

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Source: -Imperva 2019 Cyberthreat Defense Report

In order to achieve these improvements and more, organizations worldwide are increasing their spending [80]. However, information security spending numbers show there are many differences across sectors and company sizes. 53% confirm an increase in their budget [81].

V. Discussion and Conclusion

There are several other IoT security papers published, but not that most have discussed IoT security relation to the recent IoT demand. Our research looked at stable IoT connectivity standards as well as emerging IoT security patterns. A compact hierarchical protocol with cognitive shielding of private keys is supported by an encoded authentication architecture and labeling. IoT protection & privacy concerns gained a tremendous amount of interest from the scientific communities and were discussed at various levels. Explored IoT protection and privacy problems. the implementation of IoT protection and the solutions proposed for them. For embedded systems, a quick and easy encryption scheme has been developed. Second, the numerous sorts of IoT attacks were mentioned (physical, remote, local, etc.). Third, they concentrate on the frameworks and classification and applied for the purpose of access control and permission. Finally, at various layers, they examine security problems malware detection, to reinforce the protection of IoT devices, access control, authentication, and secure congestions of methodologies utilizing machine learning have also been recommended. In this area, as we discussed in the obstacles segment, believe across agents is problematic for protecting IoT devices. As the devices communicate with other devices deployed by another vendor, only authorized systems would be able to sync and relay data to either of the parties. For trust to be created, devices must have a unique identity. An IoT confidence management system that also proposed a machine learning-based design for that Since IoT devices might be free to invade and leave the system at any time, flexible confidence as in IoT framework is possible. Another new environment whereby program that facilitates artificial intelligence and machine learning manages networking and resources is system automation and purpose-based networking. An interesting field of research could be the association of software-defined networking among intended-based networks to improve network performance with enhanced usability. This is a modern field of study, so standardization is imperative. The use of intended-based networking for IoT devices and security together with SDN is indeed an open area of research. Future Work Protection is an essential concern with IoT, as we've seen, and as IoT expands to a variety of markets and utilities, such as factories, administration, and body guards, it will become increasingly essential to preserve confidential information and information systems from risk.

Reference

[1] Tarun Dhar Diwan, Dr. Siddhartha Choubey, , Dr.H.S.Hota "Multifactor Authentication Methods: A Framework for Their Selection and Comparison" accepted for publication in International Journal of Future Generation Communication and Networking Vol. 13, No. 3, (2020), pp. 2522–2538, ISSN: 2233-7857 (Web of Science).

[2] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "A Novel Hybrid Approach for Cyber Security in IoT network Using Deep Learning Techniques" accepted for publication in International Journal of Advanced Science and Technology ISSN:2394-5125, ISSN: 2005-4238 (Scopus indexed Journal).

[3] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, entitled "Development of Real Time Automated Security System for Internet of Things (IoT)" accepted for publication in International Journal of Advanced Science and Technology Vol. 29, No. 6s, (2020), pp. 4180 – 4195, ISSN: 2005-4238 (Scopus indexed Journal).

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[4] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "A Proposed Security Framework for Internet of Things: An Overview" presented in international Conference held on 20-22 December,2019, MTMI, Inc. USA in Collaboration with at amity Institute of Higher Education, Mauritius.

[5] Tarun Dhar Diwan,Dr. Siddhartha Choubey, Dr.H.S.Hota "Control of Public Services for Public Safety through Cloud Computing Environment" presented in international Conference held on 04-05 January,2020, Organized by Atal Bihari Vajpayee University, Bilaspur in association with MTMI, USA and sponsored by CGCOST, Raipur (C.G), India.

[6] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "A Study on Security and Data Privacy issues of IoT based Application in Modern Society" presented in international Conference held on 04-05 January,2020, Organized by Atal Bihari Vajpayee University, Bilaspur in association with MTMI, USA and sponsored by CGCOST, Raipur (C.G), India.

[7] Ezema, E., Abdullah, A., & Mohd, N. F. B. (2018). Open Issues and Security Challenges of Data Communication Channels in Distributed Internet of Things (IoT): A Survey.

[8] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.

[9] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of Things Security: a top-down survey. Computer Networks.

[10] Earls E. M., Moozakis C. (2018). Intent-based networking and network automation: A primer https://searchnetworking.techtarget.com/feature/Network-automation-and-intent-based-networking-A-primer.

[11] Doyle L. (2018). What is the relationship between intent-based networking and SDN? https://searchsdn.techtarget.com/answer/What-is-therelationship-between-SDN-and-intent-based-networking.

[12] CISCO (2018) Intent-Based Networking Building the bridge between business and IT, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-09-intent-networking-wp-cte-en.pdf.

[13] Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security Threats and Best Practices. IEEE Communications Magazine, 55(8), 211–217. https://doi.org/10.1109/MCOM.2017.1600899.

[14] Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: a survey. In I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(ISMAC), 2017 International Conference on (pp. 32-37). IEEE.

[15] Ghorbani, H. R., & Ahmadzadegan, M. H. (2017, November). Security challenges in internet of things: survey. In Wireless Sensors (ICWiSe), 2017 IEEE Conference on (pp. 1-6). IEEE.

[16] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[17] Kamble, A., Malemath, V. S., & Patil, D. (2017, February). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on (pp. 33-39). IEEE.

[18] Javdani, H., & Kashanian, H. (2017). Internet of things in medical applications with a service-oriented and security

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

approach: a survey. Health and Technology, 1-12.

[19] Grabovica, M., Popić, S., Pezer, D., & Knežević, V. (2016, June). Provided security measures of enabling technologies in Internet of Things (IoT): A survey. In Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016 (pp. 28-31). IEEE.

[20] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[21] Yassein, M. B., Abuein, Q., & Alasal, S. A. (2017, May). Combining software-defined networking with Internet of Things: Survey on security and performance aspects. In Engineering & MIS (ICEMIS), 2017 International Conference on (pp. 1-7). IEEE.

[22] Moinuddin, K., Srikantha, N., Lokesh, K. S., & Narayana, A. (2017). A Survey on Secure Communication Protocols for IoT Systems. International Journal of Engineering and Computer Science, 6(6).

[23] Hellaoui, H., Koudil, M., & Bouabdallah, A. (2017). Energy-efficient mechanisms in security of the internet of things: A survey. Computer Networks, 127, 173-189.

[24] Krishna, B. S., & Gnanasekaran, T. (2017, February). A systematic study of security issues in Internet-of-Things (IoT). In I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on (pp. 107-111). IEEE.

[25] Azni, A. H., Alwi, N. H. M., & Seman, K. (2017). Experimental research testbed for internet of things: A survey from security services perspectives. Journal of Fundamental and Applied Sciences, 9(3S), 231-244.

[26] Banerjee, M., Lee, J., & Choo, K. R. (2018). A blockchain future for Internet-of-Things security: a position paper. Digital Communications and Networks, (October 2017), 1–12. https://doi.org/10.1016/j.dcan.2017.10.006.

[27] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022.

[28] Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2017). Software Defined IoT security framework. 2017 4th International Conference on Software Defined Systems, SDS 2017, 75–80. https://doi.org/10.1109/SDS.2017.7939144.

[29] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain Based Data Integrity Service Framework for IoT Data. Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017, 468–475. https://doi.org/10.1109/ICWS.2017.54.

[30] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), (March), 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634.

[31] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI '17, 173–178. https://doi.org/10.1145/3054977.3055003.

[32] Doppler, K. (2015). 5G the next major wireless standard, 1–15. [71] Bernardos, C. J., Dugeon, O., Galis, A., Morris, D., Simon, C., & Szabó, R. (2015). 5G

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Exchange (5GEx) – Multi-domain Orchestration for Software Defined Infrastructures. Eucnc2015, (JULY).

[33] Fettweis, G., & Alamouti, S. (2014). 5G: Personal mobile internet beyond what cellular did to telephony. IEEE Communications Magazine, 52(2), 140–145. https://doi.org/10.1109/MCOM.2014.6736754.

[34] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for Internet of Things: a comprehensive survey. Security and Communication Networks, 2017.

[35] Ida, I. B., Jemai, A., & Loukil, A. (2016, December). A survey on security of IoT in the context of eHealth and clouds. In Design & Test Symposium (IDT), 2016 11th International (pp. 25-30). IEEE.

[36] Tank, B., Upadhyay, H., & Patel, H. (2016, March). A survey on IoT privacy issues and mitigation techniques. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (p. 2). ACM.

[37] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for (pp. 336-341). IEEE.

[38] Varadarajan, P., & Crosby, G. (2014, March). Implementing IPsec in wireless sensor networks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-5). IEEE.

[39] Benabdessalem, R., Hamdi, M., & Kim, T. H. (2014, December). A survey on security models, techniques, and tools for the internet of things. In Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on (pp. 44-48). IEEE.

[40] Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In Computational Intelligence and Security (CIS), 2013 9th International Conference on (pp. 663-667). IEEE.

[41] Peng, S., & Shen, H. (2012). Security technology analysis of IoT. In Internet of Things (pp. 401-408). Springer, Berlin, Heidelberg.

[42] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.

[43] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (IoT). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronics Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[44] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1(2011), 9-52.

[45] Santucci, G. (2010). The internet of things: Between the revolution of the internet and the metamorphosis of objects. Vision and Challenges for Realising the Internet of Things, 11-24.

[46] Granjal, J., Silva, R., Monteiro, E., Silva, J. S., & Boavida, F. (2008, September). Why is IPSec a viable option for wireless sensor networks. In Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on (pp. 802-807). IEEE.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[47] Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The internet of things. Scientific American, 291(4), 76-81.

[48] Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In Advanced Communication Technology (ICACT), 2017 19th International Conference on (pp. 699-704). IEEE.

[49] Mostefa, B., & Abdelkader, G. (2017, December). A survey of wireless sensor network security in the context of Internet of Things. In Information and Communication Technologies for Disaster Management (ICT-DM), 2017 4th International Conference on (pp. 1-8). IEEE.

[50] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

[51] Ramadhan, A. (2016). A survey of security aspects for Internet of Things in healthcare. In Information Science and Applications (ICISA) 2016 (pp. 1237-1247).

[52] Pawar, A. B., & Ghumbre, S. (2016, December). A survey on IoT applications, security challenges and counter measures. In Computing, Analytics and Security Trends (CAST), International Conference on (pp. 294-299). IEEE.

[53] Kraijak, S., & Tuwanut, P. (2015, October). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In Communication Technology (ICCT), 2015 IEEE 16th International Conference on (pp. 26-31). IEEE.

[54] Sharma, A., Pilli, E. S., Mazumdar, A. P., & Govil, M. C. (2016, November). A framework to manage trust in internet of things. In Emerging Trends in Communication Technologies (ETCT), International Conference on (pp. 1-5). IEEE.

[55] Nastase, L. (2017, May). Security in the Internet of Things: A Survey on Application Layer Protocols. In Control Systems and Computer Science (CSCS), 2017 21st International Conference on (pp. 659-666). IEEE.

[56] Oracevic, A., Dilek, S., & Ozdemir, S. (2017, May). Security in internet of things: A survey. In Networks, Computers and Communications (ISNCC), 2017 International Symposium on (pp. 1-6). IEEE.

[57] Deshmukh, S., & Sonavane, S. S. (2017, March). Security protocols for Internet of Things: A survey. In Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017 International Conference on (pp. 71-74). IEEE.

[58] Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17, 1313–1328. https://doi.org/10.1145/3133956.3134027.

[59] Mali, A., & Nimkar, A. (2017, September). Security Schemes for Constrained Application Protocol in IoT: A Precise Survey. In International Symposium on Security in Computing and Communication (pp. 134-145). Springer, Singapore.

[60] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

[61] Balte, A., Kashid, A., & Patil, B. (2015). Security issues in Internet of things (IoT): A survey. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4).

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[62] Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

[63] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211.

[64] Mark, R.-O. (2013). The Complete Reference: Information Security, Second Edition. McGraw Hill Education.

[65] Canedo, J., & Skjellum, A. (2016). Using machine learning to secure IoT systems. 2016 14th Annual Conference on Privacy, Security and Trust, PST 2016, 219–222. https://doi.org/10.1109/PST.2016.7906930.

[66] Garcia-morchon, O., Keon, S., Hummen, R., & Struik, R. (2012). Security Considerations in the IP-based Internet of Things draft-garciacore-security-04, (c), 1–45.

[67] Anna MG. (2017). Top 10 IoT security challenges. IBM developerWirks, https://developer.ibm.com/dwblog/2017/iot-security-challenges/

[68] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning. arXiv preprint arXiv:1801.06275.

[69] Sahoo, K. S., Sahoo, B., & Panda, A. (2016). A secured SDN framework for IoT. Proceedings - 2015 International Conference on Man and Machine Interfacing, MAMI 2015. https://doi.org/10.1109/MAMI.2015.7456584.

[70] Sadique, Kazi & Rahmani, Rahim & Johannesson, Paul. (2018). Towards Security on Internet of Things: Applications and Challenges in Technology. Procedia Computer Science. 141. 199-206. 10.1016/j.procs.2018.10.168.

[71] Santucci, G. (2010). The internet of things: Between the revolution of the internet and the metamorphosis of objects. Vision and Challenges for Realising the Internet of Things, 11-24.

[72] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1(2011), 9-52.

[73] Sardeshmukh, H., & Ambawade, D. (2017, June). Internet of Things: Existing protocols and technological challenges in security. In Intelligent Computing and Control (I2C2), 2017 International Conference on (pp. 1-7). IEEE.

[74] Fremantle, P., & Scott, P. (2017). A survey of secure middleware for the Internet of Things. PeerJ Computer Science, 3, e114.

[75] Kejun Chen, Shuai Zhang, Zhikun Li, Yi Zhang, Qingxu Deng, Sandip Ray, Yier Jin. "Internet-ofThings Security and Vulnerabilities: Taxonomy,Challenges, and Practice", Journal of Hardware and Systems Security, 2018.

[76] Ammar, Mahmoud & Russello, Giovanni & Crispo, Bruno. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications. 38. 8-27. 10.1016/j.jisa.2017.11.002.

[77] Salah, Khaled & Khan, Minhaj. (2017). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems. 82. 10.1016/j.future.2017.11.022.

[78] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Cloud) (I-SMAC), Palladam, India, 2017, pp. 32-37, doi: 10.1109/I-SMAC.2017.8058363.

[79] Manasha Saqib, Bhat Jasra, Ayaz Hassan Moon. "A Systematized Security and Communication Protocols Stack Review for Internet of Things", 2020 IEEE International Conference for Innovation in Technology(INOCON), 2020.

[80] Ahmad, Asma & Sinha, Professor G & Kashyap, Nikita. (2014). 3-Level DWT Image Watermarking Against Frequency and Geometrical Attacks. International Journal of Computer Network and Information Security. 6. 58-63. 10.5815/ijcnis.2014.12.07.

[81] Tabassum, Kahkashan & Ibrahim, Ahmed & Rahman, Sahar. (2019). Security Issues and Challenges in IoT. 1-5. 10.1109/ICCISci.2019.8716460.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731