International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 7 Issue 1, January-February 2023 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

New Threats, Existing Remedies, and Unresolved Issues Related to the Effect of New IoT Capabilities on Security and Privacy

Dr. Vishal Pareek[1], Mr. Ram Kumar Vyas[2]

[1]Associate Professor (Computer Science), Tantia University, Sri Ganganagar, Rajasthan, India
[2]Scholar, Tantia University, Sri Ganganagar, Rajasthan, India

ABSTRACT

The Internet of Things (IoT) is a rapidly gaining in popularity technology that allows actual objects, such as cars, appliances, and other household items, to interact and even speak with one another. It has been extensively employed in social applications, such as smart homes, healthcare, and industrial automation, as well as in industrial production. While delivering previously unheard-of ease, accessibility, and efficiency, IoT has recently generated serious security and privacy issues. Although more research is being done to lessen these hazards, many issues are still unresolved.

This survey first suggests the idea of "IoT characteristics" in order to better comprehend the fundamental causes of future IoT dangers and the difficulties in present research. The effects of eight IoT features on security and privacy are then covered, along with the vulnerabilities they pose, current countermeasures, and unresolved research issues. This study examines the majority of current research works connected to IoT security from 2013 to 2017 in order to demonstrate how IoT features affect existing security research and to help academics keep up with the most recent developments in this field.

How to cite this paper: Dr. Vishal Pareek | Mr. Ram Kumar Vyas "New Threats, Existing Remedies, and Unresolved Issues Related to the Effect of New IoT Capabilities on Security and Privacy" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-7 | Issue-1, February 2023, pp.675-683, URL: www.ijtsrd.com/papers/ijtsrd52754.pdf

IJTSRD52754

INTRODUCTION

The Internet of Things (IoT) applications (such as smart homes, digital healthcare, smart grids, and smart cities) have become widely used around the world as a result of the development of key IoT technologies. The number of connected devices worldwide will more than double from 20.35 billion in 2017 to 75.44 billion in 2025, predicts statistics website Statista. There seems to be agreement that the influence of IoT technology is significant and expanding, with International Data Corporation (IDC) predicting a 17.0% compound annual growth rate (CAGR) in IoT spending from $698.6 billion in 2015 to over $1.3 trillion in 2019.

As IoT applications and devices expand quickly, cyber-attacks will likewise get better and pose a bigger danger to security and privacy than ever before.

For instance, remote attackers could compromise patients' implantable medical equipment or smart cars, which could risk life safety as well as result in significant financial losses to people. Additionally, as IoT devices are increasingly employed in business, the military, and other crucial sectors, attackers have the ability to endanger the safety of the general public and the country.

For instance, several distributed denial of service (DDoS) assaults on Dyn's Domain Name System provider systems on October 21, 2016, rendered various websites, including GitHub, Twitter, and others, inaccessible. A botnet comprising several IoT devices, including IP cameras, gateways, and even baby monitors, is used to carry out this attack. Another example is the significant harm that Stuxnet, a harmful computer worm that targets industrial computer systems, caused to Iran's nuclear programme.

However, the majority of businesses and individuals are ignorant about privacy and security. Numerous Americans believe that their data has been handled in an overly optimistic manner, according to a recent

Pew Research Center research. Only 26% of Americans oppose sharing their medical records with their doctor. Nearly half of Americans consent to having their automobiles' location and speed monitored by auto insurance firms in exchange for price breaks on their policies. Additionally, because there is little consumer demand, product producers merely pay attention to integrating the essential features while ignoring potential security issues. IoT device manufacturers usually don't patch or upgrade their products until the user requests firmware updates.

IoT devices also struggle to operate complete security features due to resource and consumption limitations. IoT devices thus frequently have easy-to-use flaws (such default passwords or faults that haven't been fixed) for extended periods of time.

IoT device manufacturers, cloud providers, and researchers are trying to build security systems and protocols, to study new vulnerabilities, and to find effective ways to secure data privacy as a result of an increase in vulnerabilities, attacks, and information breaches. Even though researchers are still working on IoT security and privacy, the majority of their research is still in its early phases and is not generally applicable. There are still many unresolved issues. Many published surveys concentrate on IoT security in order to identify beneficial topics for more research and offer helpful references for researchers. The primary topics of discussion and analysis in Li et al. and Lin et al. and IoT architectural layers were existing attacks and problems. In two distinct application scenarios—the home and hospital—Fu et al. Highlighted various opportunities and possible risks. The research problems and potential solutions put out by Roman et al. and Sicari et al. were based on several security techniques, such as authentication, access control, confidentiality, and privacy. The most recent survey, released by Yang et al., presented the classification of IoT threats and summarized the key findings of earlier surveys. Although these surveys covered the majority of IoT security research, threats, and open concerns and offered some research guidance for the future, few of them explain the root reasons of research obstacles and security risks or explicitly state what new challenges IoT poses. Even though Yang et al. and Trappe et al. explored how limited battery capacity and computational power make it more difficult to secure IoT devices, many other IoT restrictions and features that affect security and privacy have not been examined.

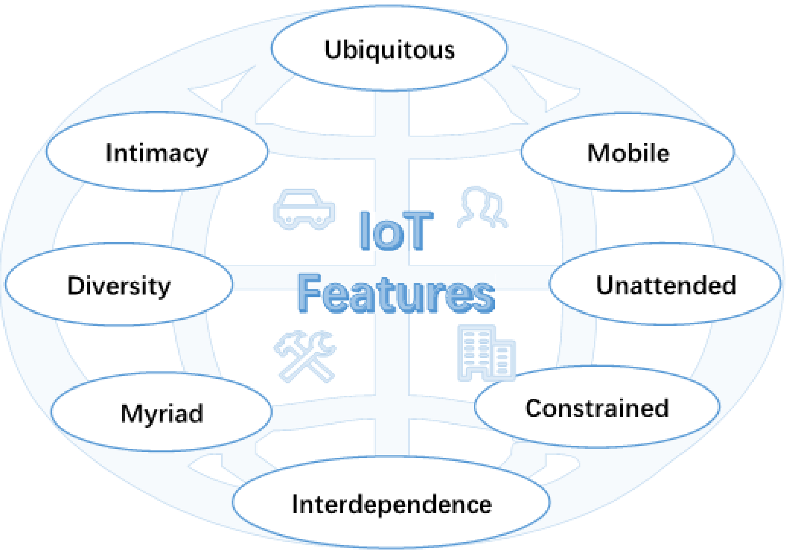

Figure 1" IoT Features

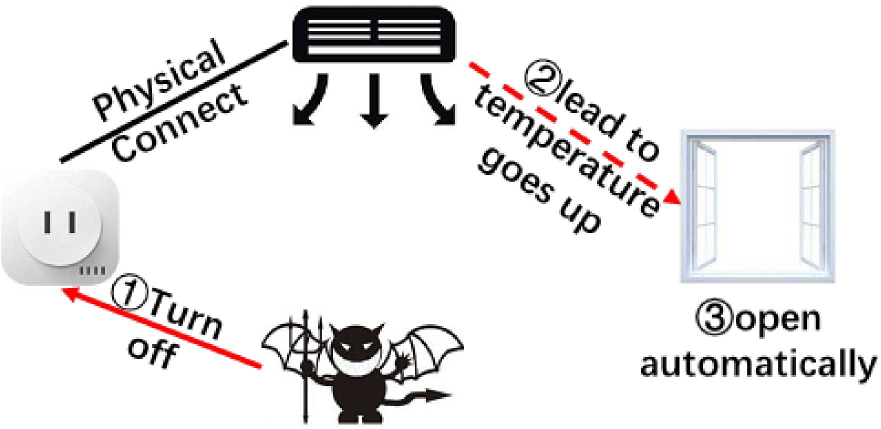

Figure 2: Attack Example of Interdependence behaviors

This paper addresses and analyses IoT security challenges from a new angle—IoT features—to close the gap. The term "IoT features" refers to the distinctive characteristics of IoT devices, networks, and applications, which differ significantly from those of smart phones and PCs. For instance, "Constrained" is an IoT feature since IoT devices have significantly less computer power, storage space, and power supply. The following is a summary of this paper's contributions:

A. We introduce the notion of "IoT features" for the first time in order to identify the underlying causes of existing risks and the major problems in IoT security research.

B. To better understand how IoT features affect security and privacy concerns, we present eight IoT features that have the greatest influence. We also explore the dangers, research problems, and opportunities derived from each feature.

C. Through the analysis of recent five years of research, we provide the trends of contemporary IoT security and its cause based on IoT features.

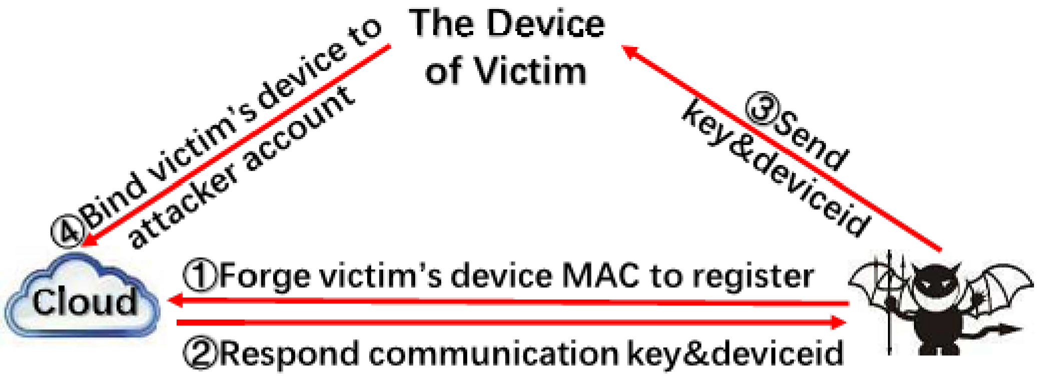
The Device of Victim
④Bind victim's device to attacker account
③Send key&deviceid
Cloud
①Forge victim's device MAC to register
②Respond communication key&deviceid

Figure 3: Device Hijacking Attack Example of JoyLink Protocols.

The rest of the document is structured as follows. The primary section of this article is Section?, where we concentrate on the eight IoT properties depicted in Fig. 1 and thoroughly explore and analyze each of them. Then, from 2013 to 2017, we gathered around 200 illustrious research papers on IoT security, and we included a variety of statistical analyses with them in Section? In Section?, conclusions are offered.

HOW IOT FEATURES AFFECT SECURITY AND PRIVACY

As illustrated in Fig. 1, we explain each IoT element in this section from four perspectives: description, threat, difficulties, solutions, and possibilities.

1. **Description:** In this section, we explain what this function is and how it differs from standard computers and mobile phones.
2. **Threat:** We talk about the weaknesses and threats that this feature might present, as well as the catastrophic repercussions that these threats could have. For some dangers, we additionally give illustrations and examples of attacks to make it simpler for the reader to understand.
3. **Challenges:** We outline the difficulties in doing research to address these concerns.
4. **Solutions & Opportunities:** We outline current solutions to the problems and dangers and talk about their shortcomings. Additionally, we present a few fresh security methods and concepts as chances that could aid in addressing the difficulties and dangers.

A. INTERDEPENDENCE

1. **Synopsis:** As IoT devices advance, their interactions grow more complicated, making human intervention unnecessary. IoT devices no longer merely overtly connect with one another like older PCs or cellphones. Many of them could also be implicitly controlled by the actions or environmental conditions of other devices using smart rules in the cloud issued by owners via the Internet, such as IFTTT, which has been widely used in IoT platforms (e.g., Samsung's SmartThings, Apple's HomeKit and Amazon's AWS IoT). For instance, if the smart plug detects the air conditioner is turned off and the thermometer determines that the internal temperature has risen beyond the threshold, the windows will automatically open. Similar examples are more prevalent in industrial and agricultural devices (e.g., automatic adding more water into smelters according to temperature and humidity). We refer to this implicit dependency relationship between devices as an IoT characteristic called "Interdependence" in this context.

2. **Threats:** Although the target system or device itself could be difficult to penetrate, attackers could simply alter the environment or the actions of other devices that are interdependent with the

target system. As a result, this functionality could be abused by attackers to circumvent the initial defensive system and make it easier to direct attack the target devices. For instance, going back to the scenario given in the previous sentence, the attacker is not required to assault the thermometer or the automatic window control directly. As seen in Fig. 2, he could use the smart plug that was linked to the public network to disable the air conditioner in a room, cause the temperature to rise, prompt the automatic opening of the windows, and result in a physical security breach.

3. **Difficulties:** The majority of researchers are unaware of how interdependent actions affect IoT security.

The one device itself is typically protected by researchers. However, because of their interdependent behaviours, it is challenging to create a distinct protective border for IoT devices or to apply static access control and privilege management techniques to them.

It is also challenging to provide a specific set of fine-grained permission rules for IoT devices since their behaviour may be affected by other IoT devices or ambient factors. Thus, the overprivilege issue has emerged as a prevalent issue in the authorization architecture of apps running on existing IoT platforms.

4. **Solutions and Opportunities:** The Carnegie Mellon University team recognized the cross-device dependencies early on and developed a set of new security principles for identifying dependency abnormal behaviour. With more devices on the market, these regulations will become increasingly convoluted and unworkable. ContexIoT is a brand-new context-based permission framework for IoT systems that Yunhan et al. introduced last year to address the over privileged issue. Prior to each device's behaviour being executed, it captures and compares additional context information such as procedure control flow, data source, and runtime data, and then allows the user to accept or reject this behaviour in accordance with the recorded information. That could identify interdependent behaviours of IoT device misuse. It is difficult to fake the same context information, even if attackers act inappropriately in identical physical conditions to the norm. However, this approach depends too heavily on user choices; if the user makes a bad choice, the system will remember it and won't question them again. To combat the risks brought on by interconnectedness, more practical and effective solutions are urgently required.

B. DIFFERENCE

1. **Description:** Heterogeneous IoT devices are built for various specific activities and interact strongly with the various physical environments in order to better accommodate various application situations. The hardware, system, and

These processes have certain requirements. For instance, a tiny temperature sensor might function on a single MCS-51 chip with minimal flash and RAM, yet the performance of an autonomous industrial machine is superior to that of our Smartphone. However, various application contexts also call for various communication protocols. Different IT businesses utilize various wireless access, authentication, and communication protocols for their smart home platforms, even within the same application, such as the smart house (e.g., Amazon's AWS IoT, JD's Joylink, and Alibaba's Alink). We refer to the occurrence that many various types of IoT devices and protocols arise in the current IoT industry as a "IoT feature" called "diversity."

2. **Dangers** The Ali mobile security team discovered that more than 90% of IoT device firmware has security vulnerabilities like hard-coded keys and common Web security vulnerabilities, which could be easily used by attackers. This is because many different new IoT device types lack adequate safety checks before release.

For novel IoT services like IoT device bootstrapping, there is a dearth of actual security knowledge, which means that new protocols frequently have many potential security issues. For instance, Liu et al. discovered that the attacker might take advantage of many Joy link protocol flaws, such as the inadequate device authentication depicted in Fig. 3. Additionally, because different protocols have distinct semantic definitions, attackers may exploit this fact to discover security flaws like Bad Tunnel when they improperly cooperate.

3. **Obstacles:** In terms of system security, the variety of IoT devices makes it challenging to provide a common system defense for the heterogeneous devices, particularly in the industrial sector. Therefore, it is vital to address how to find and address the numerous security flaws present among the various IoT devices.

Because each protocol differs from the others in terms of network security, it is important for researchers to identify their most significant generic security flaws. Additionally, researchers should take into account not only the security issues with a single protocol but also any potential security threats linked to other protocols.

4. **Alternatives & Possibilities:** Researchers conducted static or dynamic analysis on the device firmware and source code to identify and address the potential vulnerabilities for more IoT devices. A framework to facilitate dynamic security analysis for various embedded systems' firmware was proposed by Zaddach et al. in 2014. The emulator must transmit action from the emulator to the device via a physical link in order to fully imitate the operation of real devices. As a result, it is inappropriate for extensive automated firmware examination. A framework for extensive automated firmware dynamic analysis was described by Chen et al., although it can only be used with Linux-based systems. For the Real-Time Operating System (RTOS) and four bare-metal platforms, the firmware dynamic analysis simulation framework is essentially empty.

To safeguard various types of devices on the same network, other researchers rely on intrusion detection systems (IDS) and intrusion prevention systems (IPS). Attacks vary from one another, though, depending on the target gadget.

Therefore, several experts noted that when the network contains a wide variety of devices, the IDS and IPS systems concept, which is focused on anomalous traffic detection, may not operate well. They recommended that the major task of the IDS and IPS systems should be the detection of abnormal parameters that affect the actions of the devices. For instance, Hadziosmanovic et almethod.'s of detecting whether a parameter was outside of acceptable bounds allowed them to identify prospective attacks. According to Sullivan et al., the legal parameter range of industrial IoT devices should be further amended by qualified and experienced operators in addition to being extracted from the lawful traffic. There is still room for improvement in IDS and IPS systems for heterogeneous IoT devices.

C. RESTRICTED

1. **Description:** Due to financial constraints and environmental restrictions, many IoT devices, particularly industrial sensor and implantable medical equipment, have been made to be compact and light. They therefore have far less computing power and storage capacity than desktop computers or mobile phones. Many military, industrial, and agricultural devices also have strict criteria for power consumption since they must operate for extended periods of time in locations without access to charging. Additionally, a lot of IoT devices utilized in real-time healthcare systems, robot control systems, and vehicle systems must adhere to the strict time limitations of real-time processes. We define the "limited" IoT feature as the limitation of an IoT device's computing/storage resource, power supply, and latency.
2. **Dangers** Most IoT devices do not deploy the essential system and network security because of their limited feature sets.

For instance, because lightweight IoT devices lack a memory management unit (MMU), they cannot use memory isolation, address space layout randomization (ASLR), or other memory safety mechanisms. The performance of limited IoT devices is severely hampered by the implementation of the most complex encryption and authentication techniques, such as public cryptography, on such devices due to their excessive demand on computational resources. As a result, it is simple for attackers to hack these devices using memory vulnerabilities. Additionally, a lot of IoT devices even communicate with servers unencrypted or without verifying the server's certificate when using SSL encryption. Attackers might easily launch a man-in-the-middle (MITM) assault or intercept conversations.

3. **Obstacles**: Researchers face a significant issue in figuring out how to implement fine-grain system security on lightweight IoT devices with less system software and hardware. Such system protections must also be in compliance with time and power restrictions in real-world application scenarios. Additionally, it is challenging for researchers to implement more advanced encryption and authentication methods on small IoT devices with less latency and CPU power.
4. **Alternatives & Possibilities:** Previous research have focused on building system security methods for lightweight devices to improve system security for restricted IoT devices, but the majority of them are still unable to meet both the security and application requirements. On small embedded processors, ARMor, a lightweight software fault isolation, can be utilized to safeguard important application code; nonetheless, it resulted in substantial performance overhead for some programmes that repeatedly verify the address (e.g. string searching). Therefore, real-time IoT devices cannot use it. For lightweight devices, Koeberl et al. proposed a number of trusted computing features, including trusted execution and attestation.

It cannot, however, be immediately applied to existing IoT devices because its implementation requires changing the MCU's existing hardware architecture. Other system defenses, such as EPOXY and MINION [38], have recently been presented and are better suited to handle the aforementioned issues. However, they must be properly set based on static code analysis of each firmware or source code before usage, adding to developers' workloads.

Most cryptology researchers reduce resource consumption by creating new, lightweight algorithms or optimizing the current cryptography algorithms to protect network security for restricted IoT devices. However, it is challenging for lightweight algorithms to achieve the same level of security as traditional algorithms. To overcome this problem, several researchers experiment with novel approaches. For instance, the authentication and key generation technique presented by Majzoobi et al. and Hiller et al. are both based on physical unclonable functions (PUF), which leverage the particular physical structure of the device to identify it. This approach can successfully fend against side channel analysis in addition to reducing the need for key storage space and streamlining the key generation algorithm. Other researchers attempted to enhance authentication algorithms by using users' distinctive biological traits, such as gait and usage patterns, which were gathered by some IoT devices. At the same time that it can save storage and authenticate the user and the device. But physical traits or biometrics don't always follow the same trend. Unpredictable factors might cause a little alteration in them. These new techniques still need to have their accuracy and stability further refined.

D. MYRIAD

1. **Summary:** As IoT devices proliferate quickly, the amount of data they generate, transmit, and use will increase to stratospheric levels. We refer to the massive quantity of IoT devices and data here as an IoT feature called "Myriad."
2. **Dangers** The Mirai botnet, which had more than a million IoT devices, generated attack traffic in 2016 that topped 1Tbps, a feat never before accomplished by a cyber attack. Additionally, a growing number of new botnets, such as IoTroop [47], are being created primarily via unprotected IoT devices rather than PCs or smartphones. As a result, they are spreading considerably more quickly and might be used to execute massive distributed denial of service (DDoS) attacks. Large-scale DDoS attacks are the most distant network attacks, according to research by Yin et al. who developed a honeypot and sandbox system to collect attack samples from IoT devices. As more public and industrial infrastructures are connected to the Internet, IoT botnets will start to attack these key facilities as well as websites, which will have a serious negative impact on social security.
3. **Difficulties:** The majority of IoT devices lack system defense and intrusion detection technologies, such as antivirus software. IoT devices are also numerous and have a very limited power supply and computing resource, as we have already stated. Researchers face a significant issue in figuring out how to identify and combat IoT botnet viruses in IoT devices. The spread of IoT botnets must also be stopped, which is a challenging issue.
4. **Solutions & Opportunities:** By examining the Mirai's features, many researchers have attempted to identify IoT botnets. For instance, JA Jerkins et al. developed a method to identify potential vulnerabilities in IoT devices by extracting multiple attack routes from the Mirai botnet.

There were few suggestions for practical ways to stop botnet viruses. When identifying malicious requests in a sensor network, Zhang and Green first took the limits of the devices and surroundings into consideration. Their attack premise is oversimplified, though. Attackers are less likely to send requests with identical content than they are to spoof legitimate requests from regular users with different, logical material. Additionally, the existing DDoS intrusion detection techniques are only used in specific situations, such as smart grid or networks that use a particular protocol, such as 6LoWPAN.

E. UNATTENDED

1. **Summary:** Smart metres, implanted medical devices (IMDs), and sensors in specialized industrial and agricultural an extended amount of time without physical access in a military situation. These gadgets are becoming Internet of Things (IoT) devices as a result of growing popularity of wireless networking. The IoT feature "unattended" here refers to the status of IoT devices that have been left unattended for a long time.
2. **Threats physically** connecting an external interface to check the status of these devices in such environments is challenging.

   As a result, it is challenging to find the remote attacks that were directed at them.

   Furthermore, since such devices, such IMDs and industrial control devices, frequently perform critical tasks, attackers are more likely to view them as prime targets. For example, the Stuxnet worm may infect the programmable logic controllers (PLC) used in industrial control systems, causing serious bodily harm.

3. **Difficulties:** In addition to being primarily "constrained" devices, these "unattended" devices are also, as was already noted, unattended. Additionally, they are typically built to carry out very specialized functions and engage in active physical interaction. Traditional mobile trusted computing defenses for them are challenging to implement. Because so many tiny IoT devices are constructed on microcontrollers that do not support MMU, for example, process memory segregation based on virtual memory is no longer practical. As a result, creating a trusted execution environment (TEE) to guarantee that security-critical actions are appropriately carried out under remote vulnerabilities and confirming the internal state of a distant, unmanaged IoT device become vital responsibilities in many circumstances.
4. **Options and Solutions** Building a trusted execution environment for security-sensitive mobile applications using Trust Shadow makes advantage of ARM TrustZone. Defrawy et al. use a software/hardware co-design method to produce an attestation mechanism SMART with low hardware requirements, although this technology is built on the ARM Cortex-A processor and does not support small IoT devices based on lightweight processors, such as ARM Cortex-M.

However, part of SMART's access control logic involves too much time, including changing the attestation code and dealing with several protected processes. A lightweight trusted execution environment was created by Noorman et al. for tiny embedded devices; however they failed to take into account how to handle hardware interrupts and memory exceptions in a secure manner. Still unsolved issues include developing reliable and widely used remote attestation, lightweight trusted execution, and safety patch techniques.

ANALYSIS OF IOT SECURITY RESEARCH

I looked at nearly 200 research papers on IoT security from top journals and conferences according to CCF rating1 in the last five years to help researchers catch up with the most recent trend of IoT security research and better understand how mentioned features affect previous IoT security research. Then, using statistical analysis of these papers, we show how IoT security research has evolved and what has caused it. We also highlight the most recent IoT security research objectives and directions.

CONCLUSION

In this work, we examine and debate IoT privacy and security challenges from a novel angle—the IoT feature.

We highlight the security risks, current solutions, and unresolved research issues related to certain IoT characteristics. We also highlight the emerging security technologies that need more research. We conclude by illustrating the development pattern of recent IoT security research and how IoT aspects impact the existing research, based on the analysis of a wealth of priceless research. We can better identify the future research hotspots and development of the IoT security by carefully examining the impact of new IoT capabilities on security and privacy.

REFERENCES

[1] The Statistics Portal. (2017). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). [Online]. Available: https://www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/

[2] [2] IDC. (2016). Internet of Things Market Statistics. [Online]. Available: http://www.ironpaper.com/webintel/articles/internet-of-things-marketstatistics/

[3] Bigthink Edge. (2016). Hacking the Human Heart [Online]. Available: http://bigthink.com/future-crimes/hacking-the-human-heart

[4] Envista Forensics. (2015).The Most Hackable Cars on the Road. [Online]. Available: http://www.envistaforensics.com/news/the-mosthackable-cars-on-the-road-1

[5] Wikipedia. 2016 Dyn cyberattack. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=76 3071700

[6] Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy 9.3(2011):49-51.

[7] Richard Patterson. (2017). How safe is your data with the IoT and smart devices. [Online]. Available: https://www.comparitech.com/blog/information-security/iot-data-safetyprivacy-attackers/

[8] GeekPwn. (2017). IoT devices have a large number of low-level loopholes. [Online]. Available: http://www.sohu.com/a/129188339_198147

[9] Li, Shancang, T. Tryfonas, and H. Li. "The Internet of Things: a security point of view." Internet Research 26.2(2016):337-359.

[10] Lin, Jie, et al. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications." IEEE Internet of Things Journal., vol. 99, p1 2017.

[11] Fu, Kevin, et al. (2017). Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things. Technical Report. Computing Community Consortium. [Online]. Available: http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Securityand-Privacy-Threats-in-IoT.pdf.

[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Comput. Netw., vol. 57, no. 10, pp. 2266–2279, 2013.

[13] Sicari, S., et al. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks the International Journal of Computer & Telecommunications Networking 76.C (2015):146-164.

[14] Yang, Yuchen, et al. "A Survey on Security and Privacy Issues in Internet-of-Things." IEEE Internet of Things Journal 4.5(2017):1250-1258.

[15] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," IEEE Security Privacy, vol. 13, no. 1, pp. 14–21, Jan./Feb. 2015

[16] Linden Tibbets and Jesse Tane. (2012). IFTTT. [Online]. Available: https://platform.ifttt.com/

[17] Samsung. (2014). SmartThings. [Online]. Available: https://www.smartthings.com/

[18] Apple. (2014). HomeKit. [Online]. Available: https://developer.apple.com/homekit/

[19] Amazon. (2012). Alexa. [Online]. Available: https://developer.amazon.com/alexa

[20] Fernandes, Earlence, J. Jung, and A. Prakash. "Security Analysis of Emerging Smart Home Applications." Security and Privacy IEEE, 2016, pp. 636-654.

[21] Yu, Tianlong, et al. "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things." ACM Workshop on Hot Topics in Networks, 2015, pp. 5.

[22] Jia, Yunhan Jack, et al. "ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms." Network and Distributed System Security Symposium 2017, pp. 1-15.

[23] JD. (2015). Joylink. [Online]. Available: http://smartdev.jd.com/

[24] Alibaba. (2015). Alink. [Online]. Available: https://open.aliplus.com/docs/open/

[25] Alibaba. (2015). Internet of things security report. [Online]. Available:https://jaq.alibaba.com/community/art/show?articleid=195

[26] Network Working Group Internet-Draft. (2017). Secure IoT Bootstrapping: A Survey. [Online]. Available: https://tools.ietf.org/html/draftsarikaya-t2trg-sbootstrapping-03

[27] Liu, Hui, et al. "Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home Devices." IoT Security & Privacy Workshop 2017, pp. 13-18.

[28] Yang Yu. BadTunnel: NetBIOS Name Service spoofing over the Internet [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Yu-BadTunnel-How-Do-I-Get-Big-Brother-Power-wp.pdf

[29] Rubio-Hernan, Jose, J. Rodolfo-Mejias, and J. Garcia-Alfaro. "Security of Cyber-Physical Systems." Conference on Security of Industrial Control- and Cyber-Physical Systems Springer, Cham, 2016, pp. 3-18.

[30] Davidson, Drew, et al. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution." USENIX Security Symposium. 2013, pp. 463-478.

[31] Zaddach, Jonas, et al. "AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares." NDSS. 2014.

[32] Chen, Daming D., et al. "Towards Automated Dynamic Analysis for Linux-based Embedded Firmware." Network and Distributed System Security Symposium. 2016.

[33] Hadžiosmanovi´ c, Dina, et al. "Through the eye of the PLC." The, Computer Security Applications Conference 2014, pp. 126-135.

[34] Sullivan, Daniel T., and Edward J. Colbert. Network Analysis of Reconnaissance and Intrusion of an Industrial Control System. No.

ARL-TR-7775. Computational and Information Sciences Directorate, US Army Research Laboratory Adelphi United States, 2016.

[35] Zhao, Lu, et al. "ARMor: fully verified software fault isolation." Proceedings of the International Conference on Embedded Software IEEE, 2011:289-298.

[36] Schulz, Patrick Koeberl Steffen, Ahmad-Reza Sadeghi, and Vijay Varadharajan. "Trustlite: A security architecture for tiny embedded devices." EuroSys. ACM, 2014, pp: 1-14.

[37] Clements, Abraham A., et al. "Protecting Bare-Metal Embedded Systems with Privilege Overlays." Security and Privacy IEEE, 2017.

[38] Chung, Taegyu., et al. "Securing Real-Time Microcontroller Systems through Customized Memory View Switching." Network and Distributed System Security Symposium, 2018.

[39] Guo, Fuchun, et al. "CP-ABE With Constant-Size Keys for Lightweight Devices." IEEE Transactions on Information Forensics & Security 9.5. 2014, pp. 763-771

[40] Fan, Hongfei, et al. "An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices." Conference on Computer security Applications ACM, 2016, pp.16-29.

[41] Buchmann, Johannes, et al. "High-performance and lightweight latticebased public-key encryption." Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 2016, pp. 2-9.

[42] Rauter, Tobias, N. Kajtazovic, and C. Kreiner. "Privilege-Based Remote Attestation: Towards Integrity Assurance for Lightweight Clients." ACM Workshop on IoT Privacy, Trust, and Security .ACM, 2015, pp. 3-9.

[43] Majzoobi, Mehrdad, et al. "Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching." Security and Privacy Workshops IEEE, 2012. pp. 33-44.

[44] Hiller, Matthias, G. Sigl, and M. Bossert. "Online Reliability Testing for PUF Key Derivation." International Workshop on Trustworthy Embedded Devices. ACM, 2016, pp.:15-22