Literature Review on IoT Security

Ernest Ang Cheng Han

School of Computer Science and Engineering, Nanyang Technological University

50 Nanyang Ave, 32 Block N4 #02a, Singapore 639798

ERNE0009@e.ntu.edu.sg

Abstract – The advent of Internet of Things (IoT) technologies has given rise to many novelties in the 21st century, from eco-friendly and self-driving electric Tesla cars to lifesaving IoT smoke detectors, there is no doubt this category of technology is revolutionizing everyday life and disrupting industries at unprecedented rates. However, integrating everyday items with processing and networking capabilities has consequently opened up an equally challenging problem: multitudes of attack vectors and vulnerabilities for malicious hackers to exploit. This research paper reviews and summarizes IoT Security-related publications to emphasize the urgent and dire need to develop solutions to secure IoT technologies as well as interesting proof of concepts (PoCs) to do so using technologies such as blockchain and machine learning. The research papers that were analysed and summarised can be found in Appendix I.

Keywords – IoT Security, Machine Learning, Deep Learning, Blockchain, Federated Learning, Malware

I. INTRODUCTION TO IOT TECHNOLOGY

IoT technologies broadly refer to the connection of objects around us to the internet, providing seamless communication and perhaps specialised services by these objects. The re-invention and development of novel sensor and actuator hardware makes the integration of digital communication capabilities to everyday objects possible. Simple examples and use cases to illustrate this includes the location service provided by your smartphone, or perhaps you purchased Samsung's latest Smart Fridge with Artificial Intelligence (AI) capabilities, able to generate your next grocery shopping list or drop you a reminder when essential consumables are in low quantities. Transcending beyond domestic use cases, IoT has its place in enterprise settings across multiple industries – from continuous glucose monitoring systems assisting Doctors caring for diabetic patients to providing analytics on asset tracking and product quality in supply chains, the very nature of such devices and systems built upon IoT technology and the level of automation it brings about has almost made it indispensable in certain industries. On an even greater scale, certain countries has set aside billions of dollars of their budget investing in IoT technologies for public good. One such example is Singapore and her Smart Nation Initiative which aims to harness the powers of disrupting technologies to transcend the country to the next industrial phase, Industry 4.0. To do this, there is a need for "hyperconnectivity" to efficiently collect and analyse data from different sources for subsequent application, and IoT is the very technology powering this and many other initiatives, such as the TraceTogether application utilised for contact tracing during the Coronavirus Diseases 2019 (COVID 19) pandemic.

However, IoT does not come without problems and issues: Vulnerabilities, Malware, Escalated Cyberattacks leading to information theft, device mismanagement and misconfiguration, and much more. By enhancing everyday objects such as watches or even our spectacles, we equip them with the very networking capabilities and operating systems even that hackers exploit to gain unauthorized access to. A recent red teaming attack done by a mere 11 year old from the United States of America, where he illustrated how he managed to hack into a teddy bear toy via Bluetooth during the cybersecurity conference at the World Forum 2017. Though his proof of concept only managed to control the toy's arms and legs, his demonstration illustrated how connected toys and everyday objects with such computing and networking problems had the potential to be weaponized. As a result, it is crucial that we study the problems that IoT devices face and provide solutions to prevent them. As the Internet of Things is slowly but surely transiting to the Internet of Everything, this just means that the quantity and variety of objects being equipped with powerful yet vulnerable networking capabilities just increases, widening the attack vectors hackers have to gain unauthorized access and plant malicious trojans and software to. Often this has disastrous consequences for both everyday consumers and businesses. In 2017, toy company Spiral toys left an estimated amount of over 2 million messages that were recorded by their toys exposed to anyone that was versed with the IoT search engine Shodan. According to another case study by International Business Machines Corporation (IMB), IoT security breaches costs 13.4% of the total revenues for companies with revenue under 5 million annually and tens of millions of dollars for the largest of firms. From the above 2 examples, we observe the serious need to secure our IoT technology and devices and the dire repercussions if left alone.

II. SECURITY ISSUES WITH IOT TECHNOLOGY

There are many factors contributing to the weaknesses of IoT technology which are subsequently exploited. Most researchers and scientists agree that the and interconnected nature amongst IoT devices in the IoT network exposes a large attack surface for hackers. A compromised device could be used as a pivot to target other devices it is communicating with, creating a domino effect of devices getting hacked one after another. The common use of unpatched hardware for the sensors and actuators as well as software and operating systems with Common Vulnerability and Exposure (CVE) further increases the amount of vectors exploitable by hackers.

Analysing its overall network architecture, which can be divided into 3 layers – the perception layer where the sensors and actuators are located, the network layer which provides reliable transmission between the perception layer and the application layer largely based on existing networking standards (e.g. OSI Model, TCP/IP Model) with slight modifications (e.g. Adaptation/Adoption of IP), and the application layer which provides specialized services according to the user's needs – we observe that every layer of the IoT networking architecture is vulnerable to malicious hackers. For example, IoT systems which makes use of Radio-Frequency Identification (RFID) are exposed to problems such as RFID tag cloning, RF Denial-of-Service (DoS) jamming, and packet sniffing due to the wireless nature of RFID. At the network layer, the usage of conventional network standards causes IoT systems to be vulnerable to conventional problems with networking (e.g. Distributed Denial of Service attacks (DDoS), Man in the Middle attacks (MITM)). At the application layer, multiple client-side attacks such as spear-phishing or documents embedded with malware can be used against the system's end users to plant viruses or trojans within the application.

An interesting attack vector raised by Ohood Saud Althobaiti and Mischa Dohler is possible use of quantum computers to crack the cryptographic functions and hashers used by IoT networks and systems. Quantum Computing was introduced in the 1980s by a American theoretical physicist, who suggested the use of quantum system states to perform calculations instead of the conventional computers. Quantum computing uses quantum bits (similar to how classical computing uses bits) which can exist as 0, 1 or a superstition of both 0 and 1. By doing so, multiple calculations performed by quantum computers can be executed in a single parallel computation, and it is this built-in parallelism which provides the computation power of quantum computers. Through their paper, they have proven via mathematical calculations and collaborations with other researchers and scientists, that quantum computers have the ability to crack the cryptographic functions and algorithms employed by IoT systems, such as EEA1/EIA1 (based on the SNOW 3G algorithm), EEA2/EIA2 (based on the AES algorithm) and EEA3/EIA3 (based on the ZUC algorithm), all employed in LTE-M networks, a modified LTE network adapted to the needs of IoT systems and devices. Evidently, we see how the rise of quantum computing poses new security threats to information technology infrastructure, including those which involve IoT devices and systems.

Another security issue arising from IoT technologies is the lack of standardization to ensure interoperability of IoT device and systems in terms of data sharing, communications, encryption and decryption of messages over a network, where sensors, actuators as well as other devices are able to interoperate regardless of the underlying communication technology used. A research paper by Kevin Reeves from the University of Warwick outlines popular standards used in IoT implementations today relating to cybersecurity, from IEEE 802.15.4, to BS EN 60079-10-1, to PAS 212, to IEC 62443. Security is definitely a concern during the conception and implementation of such standardization protocols especially for IoT given that IoT networking and communications has its use cases in dealing with vital and critical systems and environments. One apt example would be leveraging on IoT to control the pressure monitor in a gas container. Misconfigured standards used by IoT systems could lead to a man in the middle (MITM) attack by a hacker, causing an over-pressure of the container, and in the worst case, system failure and catastrophic explosions.

So far, we have covered issues both on the client side and server side in IoT systems which make them vulnerable to cyberattacks. Another challenge raised by Cornelius Itodo, Said Varlioglu, and Nelly Elsayed is on the perspective after a cybersecurity breach has occurred: conducting digital forensics and incident response (DIFR) on IoT systems. Conventionally, DIFR is carried out via a series of stages: from preparation, to identification, to containment, to eradication, to recovery, and finally reflections (lesson learnt). The nature and components which make up an IoT system makes DIFR more complexed and difficult to perform. For instance, most IoT devices have very volatile memory systems unlike modern computers or laptops, this makes evidence collection tricky given that investigators are unable to turn off the IoT devices recklessly and bring them back to their forensics lab for further analysis as doing so poses a greater risk of losing evidences that would otherwise have been stored in memory, not only compromising the DIFR process but also rendering the investigator liable for legal and criminal charges for evidence tampering. Furthermore, going back to the interconnected nature of IoT systems, many devices maybe implicated and have to be collected back as evidences. Should the device be connected to a cloud environment, then the investigator will also have to examine the cloud environment and cloud object storage instances. To make matters worse, certain IoT devices are not as mobile or accessible such as common electronic devices that DIFR is commonly performed on, such as CCTV cameras and Refrigerators. Imagine, how would a cybersecurity forensic investigator perform his DIFR processes on an entire house which could be an example of a big-scale smart living IoT system compromised by malicious hackers. Furthermore, the data file formats and content stored in IoT devices may also differ from traditional systems or cloud storage due to the remote nature of IoT devices. For instance, a first responder or digital forensics investigator may and will most probably encounter many different file types and data storage formats when examining a compromised smart home system.

As with all engineers dealing with securing software, IoT technologies are no exception when balancing the infamous CIA triad of cybersecurity – confidentiality, integrity, and availability. Confidentiality ensures that data, objects and resources are protected from unauthorised access. Integrity ensures that data, objects and resources are protected from unauthorised changes. Availability ensures that data, objects and resources are accessible to authorised individuals. Often, it is argued that it is difficult or even impossible to effectively achieve every element of the CIA triad as focussing on one element often comes at the expense of another. For instance, ensuring confidentiality of data security and privacy of IoT systems by using multiple encryptions, firewalls, and public-private key pairs may encroach on the availability aspect of users, where it becomes very difficult for authorised user to access data given that one slight setting misconfiguration could instantly bar them from data access. Hence, as with most software and system designs, finding the balance between confidentiality, integrity and availability is also another security-related concern dealt with developers, engineers and solution architects, in addition to having to deal with the above mentioned complexities surrounding IoT systems, such as standards, inconsistent data formats, and wide attack vectors both from the client side and server side.

III. IMPACT OF SECURITY FLAWS IN IOT TECHNOLOGY

IoT technologies are in high demand and are expected to reach an approximate total valuation of more than 1.386 trillion USD by 2026. As the internet progresses from Web 1.0, to Web 2.0, and now the rise of Web 3.0 based largely decentralised technologies and autonomy such as blockchain, IoT technologies have also evolved and progressed as well, from the Internet of Content, to the Internet of Services, to slowly but surely the Internet of Things and Everything. As this niche industry continues to grow, so does the need to secure it along with the disastrous consequences if not taken seriously and implemented properly. As analysed and well-put by Jack Whitter-Jones on his paper "Security Review on the Internet of Things", he discussed historic attack vectors and malicious activities against IoT devices, and the subsequent impact it had. One of them in particular, was the Mirai Worm – a form of IoT malware which executed DDoS attacks against a common target via the use of its Botnet. This worm affected large internet providers and technology firms, such as Deutsche Telekom – a German Internet Service Provider (ISP), KrebsonSecurity, and DynDNS – one of the largest provider of Domain Name Services (DNS). An approximate 0.9 million routers were taken offline and millions of users and dependencies were affected as a result of the distribution of this IoT specific malware. Though the financial damages were not calculated or indicated in his report, one can only assume and imagine the great amount of disruptions felt by the relevant businesses and firms using the affected IoT devices. An analysis by Cloudflare, an American Multinational Technology Corporation, estimates that the Mirai Botnet would cost users with infected devices an additional USD $15 – 20 a month per device. Berkeley Researchers estimated the financial damages to KrebsonSecurity by the worm to amount to a total of USD$323,973.75.

Another paper written by Asma Zahra and Munam Ali Shah on "IoT based ransomware growth rate evaluation and detection using command and control backlisting", they highlighted the rapid growth of ransomware highly relatable and targeted to IoT technologies and devices, specifically addressing 5 rising major ransomware affected by IoT devices – CyrptoWall, Locky ransomware, Cerber ransomware, CBT-Locker, and TelaCrypt, with a 670% increase in incidents for CrptoWall and a 350% increase in incidents for the Locky ransomware. Ransomwares belong to a category of malware which encrypts files on devices and demands a ransom in exchange for decrypting the files. These attacks caused an estimated damage of 92 million pounds in the United Kingdom, while the worldwide financial damage inflicted amounted to a total sum of US$ 4 billion. Just as how the IoT technologies has evolved with the progression of the world wide web, so have ransomwares, as seen in the case of FLocker – an Android mobile lock-screen ransomware that was adapted to work on Smart Televisions. The abovementioned exploits and malware are just one of the few many examples of the need to secure our IoT devices and the severe consequences and repercussions if we do not. From financial damages, to personal data leaks, it is clearly instrumental that software development firms and even hardware development firms relating the IT systems regularly audit their systems and invest considerable amount of resources securing their infrastructure and also training employees to not fall for common client side attacks which occur at a greater likelihood compared to server side vulnerabilities. In the following section, apart from these common mitigation strategies, we will be focussing and discussing more novel threat detection and response strategies and proof-of-concepts to counteract the common and new security threats to IoT technologies as previously discussed in Part II of this review. Solutions such as deep neural networks based on federated learning for threat intelligence and the usage of immutable ledgers from Blockchain for ensuring data integrity will be explored and evaluated to see how they can be leveraged upon to secure our IoT technologies and devices.

IV. SOLUTIONS TO SECURING IOT TECHNOLOGIES

Securing our IoT devices can occur at various levels. For this section, will be evaluating current and novel solutions in protecting our IoT-based infrastructure from 4 points of view: Hardware-level solutions, Operating System-level solutions, Software-level solutions, and People/Policy-level solutions. Additionally, we will be analysing the current weaknesses and limitations of said solutions and proposed future development ideas to further harden and protect our IoT devices and infrastructure.

Hardware-level solution: Multiple security enhancements have long been proposed by firmware engineers that can possible hardened IoT devices' defences from vulnerabilities and malicious software. The microcontroller is the heart of most IoT devices in the edge computing layer – also the layer with the sensors and actuators and hence making it the layer with the most amount of hardware. A common methodology in improving the security capabilities of microcontrollers and such embedded systems of IoT edge devices is through using a Trusted Execution Environment (TEE). TEEs are tamper-resistant computing environments that run in a separate kernel from the IoT device. TEEs ensure the authenticity of any programs ran on the IoT device as well as the integrity of important components of the operating system and firmware system. Some TEE modules designed for microcontrollers are ARM TrustZone, Intel Software Guard Extension (SGX) and Samsung KNOX, and most of which provide a low-level application programming interface for engineers to interact and utilize the module and can hence be customized according to the IoT infrastructure it is being used for.

Limitations: TEEs and other hardware-based solutions do not address many modern hardware viruses and malware such as Hardware Trojans and Booting Vulnerabilities. Currently, TEEs do not provide any clear and concrete defence mechanisms against such hardware exploits which could have the potential to access debug ports and on-chip embedded systems and thus grant hackers unauthorised access to confidential assets or data within the edge device. This applies to the boot process and many other hardware-related components which make the IoT device itself vulnerable to cyberattacks such as Code Injection vulnerabilities or Node Capture attacks.

Improvements: Future development in embedded systems and hardware components such as microcontroller parts can and should be expected as they are required not only in IoT devices and technologies. One example would be perhaps the implementation of Physical Unclonable Functions (PUFs) – physical objects that serve as unique identifiers, usually for semiconductor components such as microprocessors and microcontrollers, often serving in secured communications and authentication. Given its nature, PUFs are a great addition to the IoT ecosystem of hardware which can be used to provide additional security to IoT devices. Another possible development opportunity would be the integration of hardware firewalls on to more IoT devices' components apart from the current ones such as the System-on-a-Chips (SoC) and the Network-on-a-Chips (NoC).

Operating System-level solution: OP-TEE is an example of a popular solution for enforcing and providing additional verification and authentication to processes and applications that run on the operating system. These applications are first registered as "Trusted" before being stored and ran in a single thread within the OP-TEE operating system space. Any calls or requests made to access or edit the applications will be done via the OP-TEE's exposed API, resulting in the fact that the program along with any other dependencies, files or data will never be directly touched by even authorized users, let alone malicious applications. These external entities will only interact with the well encrypted OP-TEE interface running in parallel with the host operating system kernel.

Limitations: TEEs are excessively used especially in mobile devices. Additionally, the organisation and registration of Trusted Applications (TA) based of the OP-TEE framework has proven to be vulnerable to memory corruption, allow malicious actors to hijack the control flow of these applications running and even gain arbitrary code executions within the operating system space. Researchers have studied and open-sourced these vulnerabilities as well as their corresponding exploits, ranging from Stack-based buffer overflows, to Type-Confusion bugs and Shellcode Injection into the system's memory space.

Improvements: Memory protections programs such as TrustShadow and CryptMe, could be possibly integrated into Operating systems to provide another layer of support to the OP-TEE processes running in parallel and thereby hardening its defences from memory corruption. These programs aim to maintain execution environments and provide memory protection for applications. In our context, we could leverage these processes to prevent memory corruption to the TAs on our OP-TEE system as well as ensure the proper functioning of the very execution environments, preventing malicious actors from attacking and controlling the kernel. It is possible to extend this memory protection scheme to the entire computer system and cover every process and application within it. Operating systems such as Bear OS are small enough to be loaded into its own on-chip memory (OCM) allowing it to have the capabilities to encrypt all code and data outside the chip boundary at section granularity.

Software-level solution 1: The rise of new technologies such as machine learning and blockchain also provides novel solutions in the cyberspace and also IoT technologies. Intrusion Detection Systems can be equipped with threat intelligence and detection capabilities based off deep learning and a fog-to-node method of generating huge volumes of data given the massive size of an IoT network. Machine learning also value adds in research and analysis of data regarding historical and past cyberattacks. K-Means Clustering and other unsupervised learning algorithms help to study possible patterns of malicious actors, mining out rules and regulations along with the detection of relevant patterns.

Limitations: An essential component of any machine learning model would be the availability of data for training, validation and testing. This significant amount of IDS-related datasets targeted at IoT devices or IoT technologies are lacking. There is an urgent need for newer and more comprehensive datasets which consists of a wider range of IoT malware activities given the novelty of cyberattacks and hence, generating machine learning models based on old threats and datasets such as DARPA or KD99 may not be competent enough to detect newer malware activity such as zero-day exploits and complicated computer viruses.

Improvements: Apart from lacklustre datasets, the robustness of these machine learning models still need further verification and improvement in terms of their ability to predict and detect malicious software and unauthorised intrusions. Various obfuscation techniques can be and are usually applied by hackers to hide their malware through concealment techniques such as encryption, packing and steganography which can easily bypass current threat intelligence deployments. A reliable IDS powered by machine learning for IoT infrastructure must encompass the following criteria: have low false positives, high adaptiveness to extreme communication systems and unexpected behaviour from sensors, as well as the detection of zero-day vulnerabilities.

Software-level solution 2: On the other hand, we have blockchain which has risen to fame and popularity with the advent of Web 3.0 and decentralisations. With a wide span of use cases, securing IoT devices are one of them. For instance, smart contracts can be used to store and transmit data instead of common message broker protocols such as Message Queue Telemetry Transport. Through this, packets are encrypted via complicating hashing and encoding performed by Ethereum which would otherwise be exposed via Man in the Middle attacks (MITM) using software such as Wireshark. Another use case and functionality that blockchain provides to IoT ecosystems is in the area of maintaining data integrity through the use of its immutable ledger. The peer-to-peer decentralised system of the blockchain ledger ensures that any data added to it cannot be changed or altered once it is recorded onto the network which can be used to ensure data integrity and prevent malicious actors from altering or changing data on a decentralised network.

Limitations: Blockchain ecosystems require great quantities of power and electricity to facilitate transactions and maintenance, power which IoT devices will definitely lack given the minute and compact size of their storage and processing power. According to a research conducted by the Cambridge Center for Alternative Finance (CCAF), bitcoin, a cryptocurrency built on blockchain, consumes an average of 110 terra-watts of electricity annually. Furthermore, the storage capacity needed by sensors and actuators are much smaller compared to ledger based blockchain technology. A traditional IoT infrastructure stores data in a central server where as a blockchain ecosystem stores a ledger at each node within the system, necessitating bigger storages which IoT devices may be uncapable to provide.

Improvements: Blockchain developers and decentralised system engineers could research the optimization of blockchain and blockchain-based platforms before creating a blockchain which requires lesser energy consumption and storage requirements. Apart from designing cost-efficient lightweight blockchain networks, we need to continue to monitor the everchanging threat landscape and adapt blockchain technologies as solutions to these arising problems. For example, how could engineers design a blockchain to reduce the possibility of tampering not only the software of IoT devices but also the hardware? Another circumstance to consider would be ensuring the data privacy and integrity within IoT devices using blockchain given its decentralised nature in the situation whereby the device is physically stolen and taken away by hackers for further elaborate injections and malware insertions later.

V. CONCLUSION

IoT technologies are on the rise and are here to stay. Understanding the needs and trends of IoT device and infrastructure use cases is instrumental to identifying possible flaws within the system and hardening its defences. The advent of other novel technologies ranging from quantum computing capabilities to decentralised blockchain systems can serve both as a double-edged sword: either to penetrate and crack existing IoT security systems or to further enhanced them. System engineers and business entrepreneurs venturing into this space of technology must put in equal amount of resources in both the development of IoT driven products as well as cybersecurity systems, for if not, the consequences would be catastrophic – huge volumes of data leakage, cyber infrastructure damage worth millions of dollars, and even physical damage and maybe even the loss of human life.

VI. REFERENCES

[1] Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019). CyberSecurity: A review of internet of things (IoT) security issues, challenges and techniques. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS).

[2] Althobaiti, O. S., & Dohler, M. (2020). Cybersecurity challenges associated with the internet of things in a post-quantum world. IEEE Access: Practical Innovations, Open Solutions, 8, 157356–157381. https://doi.org/10.1109/access.2020.3019345

[3] Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149–160. https://doi.org/10.1016/j.dcan.2017.10.006

[4] Bao, J., Hamdaoui, B., & Wong, W.-K. (2020). IoT device type identification using hybrid deep learning approach for increased IoT security. 2020 International Wireless Communications and Mobile Computing (IWCMC).

[5] Biswas, A. R., & Giaffreda, R. (2014). IoT and cloud convergence: Opportunities and challenges. 2014 IEEE World Forum on Internet of Things (WF-IoT).

[6] Dalal, K. R. (2020). Analysing the role of supervised and unsupervised machine learning in IoT. 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC).

[7] Dlamini, N. N., & Johnston, K. (2016). The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review. 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE).

[8] Dorasamy, M., Joanis, G. C., Jiun, L. W., Jambulingam, M., Samsudin, R., & Cheng, N. J. (2019). Cybersecurity issues among working youths in an IoT environment: A design thinking process for solution. 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS).

[9] Fleischer, F., Busch, M., & Kuhrt, P. (2020). Memory corruption attacks within Android TEEs: A case study based on OP-TEE. Proceedings of the 15th International Conference on Availability, Reliability and Security.

[10] Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K., & Nijdam, N. A. (2020). A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. 2020 IEEE International Conference on Blockchain (Blockchain).

[11] Goswami, S. A., Padhya, B. P., & Patel, K. D. (2019). Internet of things: Applications, challenges and research issues. 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).

[12] Grammatikakis, M. D., Papadimitriou, K., Petrakis, P., Papagrigoriou, A., Kornaros, G., Christoforakis, I., & Coppola, M. (2014). Security effectiveness and a hardware firewall for MPSoCs. 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS).

[13] He, Z., Yin, J., Wang, Y., Gui, G., Adebisi, B., Ohtsuki, T., Gacanin, H., & Sari, H. (2021). Edge device identification based on federated learning and network traffic feature engineering. IEEE Transactions on Cognitive Communications and Networking, 1–1. https://doi.org/10.1109/tccn.2021.3101239

[14] Itodo, C., Varlioglu, S., & Elsayed, N. (2021). Digital forensics and incident response (DFIR) challenges in IoT platforms. 2021 4th International Conference on Information and Computer Technologies (ICICT).

[15] K, S. K., Sahoo, S., Mahapatra, A., Swain, A. K., & Mahapatra, K. K. (2017). Security enhancements to system on chip devices for IoT perception layer. 2017 IEEE International Symposium on Nanoelectronic and Information Systems (INIS).

[16] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00077-7

[17] Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140

[18] Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D. (2019). Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. IEEE Access: Practical Innovations, Open Solutions, 7, 9368–9383. https://doi.org/10.1109/access.2018.2890432

[19] Nehal, A., & Ahlawat, P. (2019). Securing IoT applications with OP-TEE from hardware level OS. 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA).

[20] Nzabahimana, J. P. (2018). Analysis of security and privacy challenges in Internet of Things. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT).

[21] Poyner, I. K., & Sherratt, R. S. (2018). Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people. Living in the Internet of Things: Cybersecurity of the IoT - 2018.

[22] Reeves, K., & Maple, C. (2018). IoT Interoperability: Security considerations and challenges in implementation. Living in the Internet of Things: Cybersecurity of the IoT - 2018.

[23] Roopak, M., Yun Tian, G., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC).

[24] Saeed, S., Jhanjhi, N. Z., Naqvi, M., Humayun, M., & Ahmed, S. (2020). Ransomware: A framework for security challenges in internet of things. 2020 2nd International Conference on Computer and Information Sciences (ICCIS).

[25] Salih Mohammed, M. H. (2021). A hybrid framework for securing data transmission in internet of things (IoTs) environment using blockchain approach. 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

[26] Soumyalatha, N., & Manjunath R, K. (2019). Key Technologies and challenges in IoT Edge Computing. 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).

[27] Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P., & Dang Hai, H. (2018). Recent challenges, trends, and concerns related to IoT security: An evolutionary study. 2018 20th International Conference on Advanced Communication Technology (ICACT).

[28] Whitter-Jones, J. (2018). Security review on the internet of things. 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC).

[29] Yadav, E. P., Mittal, E. A., & Yadav, H. (2018). IoT: Challenges and Issues in Indian Perspective. 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU).