Journal of Engineering Science and Technology
Special Issue on ICCSIT 2018, July (2018) 204 - 215

BLOCKCHAIN FOR A SECURED AND FORENSICALLY SOUND INTERNET OF THINGS

MARYAM SHAHAPASAND*, SEETARAM CHANDRASHEKHAR, SAILALITH SARUPURI, VINESH THIRUCHELVAM

Asia Pacific University of Technology and Innovation, Technology Park Malaysia
Bukit Jalil, 57000 Kuala Lumpur, Malaysia
*Corresponding Author: maryam.shahpasand@staffemail.apu.edu.my

Abstract

Internet of things (IoT) has been generating billions of data over the past few years, hence leading to the Big Data era. This huge amount of data has gained the attention of hackers. The traditional security measures for preventing and countering attacks from hackers prove to be ineffective due to new techniques from hackers and the new infrastructure of the IoT devices. Traditional digital forensic investigation processes and tools are no longer applicable. The data come in various forms, speed, and quantity. In this paper, the security and forensic issues in IoT and Big Data have been discussed. Furthermore, the necessity of applying blockchain in both security and forensic model has been elaborated. Blockchain enables the creation of a decentralized system for IoT devices and provides better security for the IoT world as well as ensures that it has forensically sound methods to trace anomalies in the tamper-proof ledger system.

Keywords: Big data, Blockchain, Confidentiality, Forensics, Internet of things, Privacy, Security.

1. Introduction

Over the last two decades, technology has made serious advancements and has resulted in the term "Internet of Things" (IoT). Chen defined IoT as the things that can collect data from the environment to send and share information over the internet without human interaction [1]. Those things can vary from the traditional equipment to common household objects such as fridges and microwave ovens. The number of connected devices connected to IoT in 2016 is around 17 Billion which have already outnumbered the World Population (7.6 Billion) [2]. Venčkauskas et al. [3] anticipated that the number will continue to grow exponentially.

Eventually having so many connected devices started to generate more and more data as time passes. IoT has given rise to Big Data along with other technologies which collect data such as Facebook and YouTube [4]. Based on a recent study, the 3V's of Big Data are: Volume, Velocity and Variety, and the study also mentioned the issues related to handling such huge amount of data [5]. In the following sections, various classification of security attacks has been discussed along with the privacy issues in IoT. Furthermore, the forensic issues in the current methods were explained together with the characteristics responsible.

2. Internet of Things and Big Data

The term 'Big Data' refers to an abstract concept of which people have different definitions. According to SAS Institute Inc., it is defined as data with enormous volume that floods a business on daily basis [6]. However, it can simply be understood as datasets that could not be captured, managed and analyzed by traditional IT infrastructure [1]. A few others have defined it as the technology that can be leveraged to extract insights from large volumes and a wide variety of data being captured at a high rate. These definitions gave way to summarize the characteristics of big data into the '3Vs', Volume, Velocity, and Variety according to SAS Institute Inc. [6].

Volume refers to the gathering and store of data in diverse disseminated data stores. The management of the volume of data has exponentially expanded. Apart from text, data also involve recordings, large graphics, and music. Terabytes and Petabytes are the current forms in which data is categorized into several businesses. Velocity is defined by the speed with respect to which data is produced and is evolved. This refers to how the undertaking of Big Data have to foster and deduce the outcome or the visualization in just a matter of seconds or milliseconds due to analytical applications. Variety deals with the diversity of the content which is a pivotal criterion in big data such that the organization of data is a must or not. Variety can be subdivided into internal or external data. The former considers the assembling of internal utilities in the association of CRM, ERP, internal databases and others.

As shown in Fig. 1 [7], there are various fields where IoT devices can fit it. The IoT paradigm has picked up popularity in the recent years [8, 9]. IoT deals with daily diverse used gadgets which can continuously relate to each other through the Internet. Furthermore, all these fields are generating a tremendous volume of data leading to Big Data. It was also pointed out that Medical services, transportation, entertainment, power grids and even smart premises are examples of various domains where IoT can be employed.

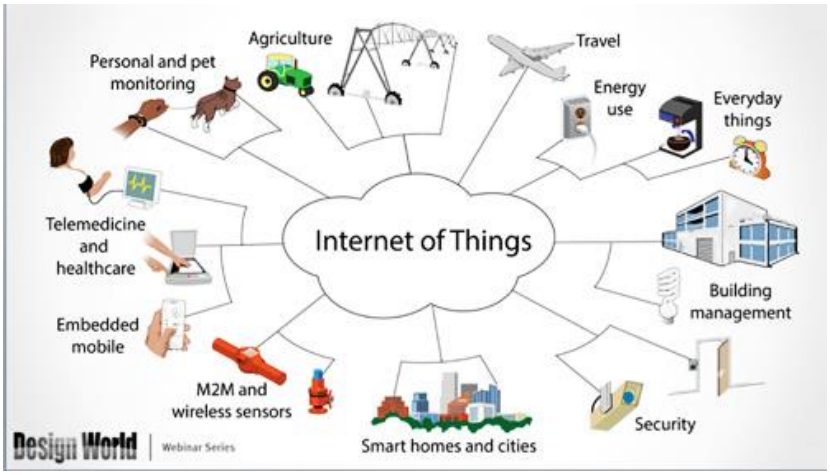

Fig. 1. IoT devices [7].

3. Security Issues

Computer security includes maintaining Confidentiality, Integrity, and Availability (CIA) in all sections of any computer system [3]. These sections consist of data, hardware, software, and firmware. Confidentiality refers to the personal information which can be read by only authorized users [10]. The system is said to have integrity if the data has not been altered, modified or tampered during the transmission since no customer will trust the system if the data is biased and keep changing [11]. Industries have adopted "Big Data" technology to be able to analyse the behaviour of customers and predict market trends. Big Data technologies such as Hadoop have brought various business advantages to the companies, but very often, companies tend to neglect the security and privacy protection when performing Big Data Analytics [12].

IoT and Big Data rely on making data available using Internet technology, but the challenge lies in doing it in a secure method so that personal data is not revealed to the Internet [11]. Furthermore, most of the IoT sensors, applications, and devices are not designed to handle security, therefore various problem concerning privacy, confidentiality, and data integrity have raised. Majority of these IoT devices are left unattended which make them an easy target for hackers to intrude into them [10].

3.1 Security attacks

Andrea et al. [13] stated that an IoT system can be attacked in many ways such as physical, network, software or encryption attacks. These attacks are discussed as follows:

3.1.1. Physical attacks

Physical Attacks requires the attacker to be near the IoT devices or inside the IoT system to operate. Kumar et al. [10] pointed out that this attack is focused mostly on the hardware devices of the IoT system and directly damages the lifespan and alter the normal usage of the device.

- Physical Damage - the attacker physically cause damage to the IoT device

- Node Tampering - this is done when the node or part of its hardware is replaced to obtain access and change sensitive information such as crypto-keys.
- Malicious Node Injection - this attack is made possible by implementing a malicious code between two nodes in the IoT system and is also known as the "Man in the Middle attack."
- RF Interference - this attack is made by creating a Denial of Service (DoS) using an RFID tag to create a noise signal and cause a disturbance in the communication.
- Unethical Manufacturer - some manufacturers make use of the public and push them to buy their cheap sensors. They secretly collect information from their customers and then sell it to the black market.

3.1.2. Network attacks

Kumar et al. [10] described network attacks as the most vulnerable and targeted layer since it carries a huge amount of data. The following attacks are the common threats to network layer:

- DOS - an attacker sends many packets of data to an IoT network more than it can handle causing an interrupt in service.
- Distributed Denial of Service (DDOS) - The attacker gets access to many unprotected IoT devices and makes them into his bots which will work under his commands. Hence all these bots will launch a series of attacks to create a DOS.
- Man in the Middle Attacks (MITM) - the attacker intercepts the data between two nodes in an IoT network and reads the data, which violate the privacy. He can control the communication between the two nodes.
- Traffic Analysis Attacks - the attacker sniffs personal information from RFID technologies since it has a wireless mode of communication.
- RFID Spoofing- the attacker impersonates a legitimate user by sending the same ID tag from RFID and get access to the system.
- RFID Cloning - the attacker makes a copy of the RFID tag by duplicating the data from a victim RFID, making him like a valid user when connecting to the IoT system.

3.1.3. Software attacks

Andrea et al. [13] described software attacks as the main origin for the security weaknesses in a computer system. The following attacks are common threats to software layer:

- Virus and Worms - The attacker inserts a virus onto the IoT system, which results in data tampering, data loss or DOS.
- Spyware and Adware - Kumar et al. [10] stated that spyware is a malicious application which monitors all the activities of a computer and sends it to the attacker to get personal information such as usernames and passwords.
- Adware is the application which displays advertisement on the computer it is installed on, usually the advertised programs are the harmful software.

3.1.4. Encryption attacks

Encryption attacks are based on cracking the encryption code and getting the key to decipher the data in an IoT system such as the Side Channel Attacks whereby the attacker makes use of specific techniques including timing, electromagnetic, power and fault analysis [13]. The attacker first must use the MITM attack to obtain the encrypted data.

3.2. Privacy issues

End-users and companies consider the benefits of IoT which facilitate their lives and ignore that they are compromising their own privacy [14]. Furthermore, some countries do not even have a privacy framework or policies for data protection. In fact, there have been cases whereby the government itself has been spying on its citizens and collecting data from computer and smartphone-users [15]. Basically, all individuals have the right to have privacy and freedom of speech. It was affirmed that when people know they are being observed, they tend to act differently and cannot express themselves freely [16]. It has always been the foundation of any service to respect the privacy right which hackers and companies take for granted and sell personal information about customers and people [16].

3.3. Recent security challenges

In the same way, as other advancing IT and Networking technologies, IoT has numerous difficulties which are exhibited below [17].

3.3.1. Security

Security is one of the fundamental concerns of any field. In IoT, environment security has a variety of scope which incorporates gadgets, network, consumer data and personal devices [18].

3.3.2. Server technologies

IoT gadgets continue developing, the extra rapid calculation is required for those gadgets that may get offloaded to servers [19]. Other applications which may assist IoT system will be available on the servers. Moreover, the patterns of IoT may affect the development of server technologies also. With greater headway in IoT, increasingly top of the line servers are expected to assume an important part.

3.3.3. Lack of shared infrastructures

IoT consists of various sensors, actuators, and software that works at the assembly level [20]. In the event of software, there are different open source devices accessible which reduce the cost of software product improvement.

3.3.4. Lack of common standards

Since IoT is a perplexing interconnection of heterogeneous sensors, actuators, and software which have their own conventions to impart and share the data. The absence of regular standard is one of the potential issues however advance is going ahead to furnish engineers to work with the standards [20].

3.3.5. Data privacy control

A huge amount of data is produced because of different IoT gadgets which may display personal user information such as data access and storage locations which requires security. This issue may prevent several users from utilizing IoT on a global level accordingly. Universal policies and guidelines should be set and arranged with respect to information protection for IoT. This will help firms from various parts of the world to trade and give their services paying little heed to their trust among the clients about the protection of their information when utilizing IoT items.

3.3.6. Sharing of data

The IoT gadget will be billions in number by 2020 future potential clients who purchase these items from various organizations will likewise increment in like manner [3]. Individual information about these clients can be exceptionally helpful to other association too. Now and then organizations give such information. This information can be utilized for different purposes like promoting, feedbacks about products or services.

4. Forensic Issues

Digital Forensics refers to the science of investigating and establishing facts leading to an incident [21]. Executing these forensic procedures in the IoT paradigm is referred to as 'IoT forensics'. IoT Forensics is a branch of Digital Forensics that deal with identification, collection, organization, and presentation in IoT infrastructures. Few characteristics of IoT solution like decentralized data need for privacy within personal networks and interaction of different communication protocols makes implementing of these forensic procedures challenging [3]. The challenge in these forensic processes is to protect the evidence since evidence is of utmost importance in handling such incidents and to develop methods for investigation. Organizations need to take proactive measures to prepare themselves for such incidents.

Though the security measures have become sophisticated, cybercrime has been evolving, and with it grows the complexity of detection and analysis. Organizations need to perform few activities to achieve the state of Digital Forensic Readiness (DFR) with an objective to improve the ability to collect evidence and reduce the cost of forensics. In IoT-based environments, activities like scenario definition, evidence source identification, planning incident detection, potential digital evidence collection, digital preservation and storage of potential evidence can be performed as a proactive process [22].

Once the evidence is collected and preserved, it is filtered based on the relevance and the ability to produce intelligence, since the quantity of data collected is huge. Different techniques like search techniques, data mining techniques, event reconstruction techniques, and timestamp analysis are used to analyze information from the data [3]. Due to the lack of common standards and an increase in proprietary technologies, and the complexity of IoT systems, the investigation process becomes quite challenging [23]. It was pointed out that the traditional tools and techniques which were once used in the investigation processes will soon become obsolete. The challenges are identified for each step of the forensic analysis process and presented below [21].

4.1. Identification

With the exponentially growing number of devices that are connected to the IoT network, the possible amount of evidence that can be collected could be huge. In a network of hundreds of devices, though one device is malfunctioning, the logs generated by all the devices must be analyzed to identify and collect evidence from the malfunctioning device [21].

4.2. Collection

Collection of evidence is an important step in the process of digital forensic investigation. Challenges in this step come due to the numerous devices connected to the network and the highly distributed nature of the network [21]. Also, different technologies and communication protocols are used on different devices. Data from these devices is usually stored in the cloud since the on-device storage is low and hence accessibility and legal issues arise while collecting data as evidence.

4.3. Organization

Collected data needs to be organized before proceeding with the further investigation process. This will help in identifying and associating relevant information from the big data collected. Lack of widely accepted protocols, and common standards as well as the existence of wide varieties of IoT structure makes evidence organization a challenge in IoT Forensics [21]. The huge volume of collected evidence also makes it a challenge, which can be addressed by using data mining techniques and tools.

4.4. Presentation

IoT systems are complicated for a human to comprehend without prior knowledge. Hence, the technicalities involved with evidence collection and the analysis can be too complicated to understand [21]. To strengthen the IoT security, blockchain, a decentralized and transparent transaction recording system could be incorporated. This would bring in an advantage to the forensic community. Since there is no centralized and trusted authority, transparency and trust are established among the entities in the network.

5. Blockchain Technology

Blockchain technology is a data structure that makes decentralized and distributed digital records of transactions in a system possible [24]. Others have defined it as a transaction database or a record-keeping technology with distributed trust mechanism in which records were linked with the previous ones and the database are shared among the entities participating in it [25, 26]. Pierro [26] stated that the main driver in inventing such technology is to establish a state of trust among the parties involved and build a system where the records cannot be tampered with, without being detected. Blockchain's mechanism is explained by using bitcoin, the first application for which blockchain laid the mathematical foundation. Bitcoin is like an online bank whereby the user maintains his account information and balance. The fundamental distinction here is the authority that maintains the transaction records.

Unlike traditional banking, users collectively maintain the ledger of the transactions. Though the information is publicly accessible to all the users, a system of a digital signature for verification, signing, and validation of transactions guarantee the information security. One half of the digital signature called the 'private key' is kept by the user and the other half called the 'public key' as the name suggests, is publicly available to all the users. For a user to make a transaction, the private key is needed to sign the transaction and other users verify the authenticity of the transaction using the public key. Once the authentication is complete, this transaction is notified to all the nodes and the record is added to the chain of transaction blocks. These records are encrypted using hash functions which makes them extremely difficult or close to impossible to tamper with. The salient features of this technology can be enumerated as follows: open and distributed record keeping, encryption of transactions to strengthen information security, tamper-proof, permanent transactions.

The following section provided an explanation of the importance of incorporating Blockchain technology to overcome the challenges in IoT.

5.1. Blockchain and IoT

Industries and researchers have identified the combination of IoT and blockchain as a disruptive mechanism that would transform across many domains. Since the control over the system is distributed, unlike centralized control in cloud-based systems, there is no single point of failure [24]. In the article, the author also demonstrated the significance of blockchain's role in strengthening the security of IoT by discussing an incident that happened in October 2016 where a US-based service DNS provider faced distributed denial of service attacks and the system was infected with malware via the IoT devices. With the intention of strengthening security, initiatives are being taken by several companies to develop a framework to incorporate blockchain into IoT.

An illustration of the architecture for IoT based on blockchain technology is shown in Fig. 2. [27] Each participating node of the blockchain networks will be able to communicate with each of the other nodes in the network. All the nodes have the same copy of the ledger or transaction data that is generated within the network. Any kind of access or update to the transactions would require a consensus from all the participating nodes. Any attempt at evidence tampering by compromising a node would be automatically invalidated by the remaining nodes of the network, thus preserving the original data.

This architecture would demand the IoT solution to be heavily equipped with hardware for storage and processing. Though blockchain technology shows promising solutions to the security issues of IoT, the practicality of the solutions where the latency for real-time transactions is concerned, is yet to be determined. The nature of blockchain already acts as a solution due to its decentralized feature and is secured against Denial of Service. Blockchain prevents data from being manipulated by insider attacks. Most companies are still unable to fully understand how blockchain works and are unwilling to take the risk of the venture in the blockchain technology. The blockchain is still being nurtured and not yet being used to its full capabilities.

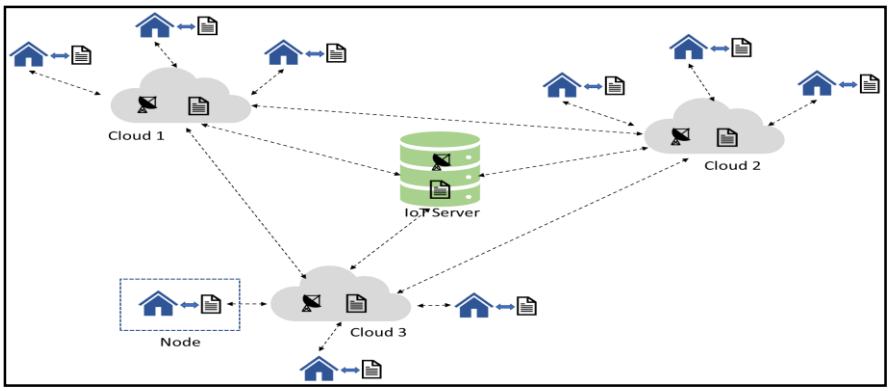

Fig. 2. An illustration of blockchain-based IoT architecture [27].

5.2. Blockchain for IoT security

Blockchain helps to maintain Confidentiality in a system by ensuring that sensitive information is not being disclosed to unauthorized parties using various authentication and authorization controls. The block of data is fully encrypted which means even when the data is flowing among untrusted network, the unauthorized parties will not be able to access it. This means only the person with proper authorization will be able to access the data and using his specific private key, he will be able to decrypt it. The PKI provides a higher level of security. Even in the scenario of the man in the middle attack, the attacker will not be able to forge the intended recipient identity [28].

Blockchain will also promote Integrity of the system by ensuring the consistency of the data by using data encryption, comparing of hashes and digital signature throughout the data lifecycle in the system. The main feature of blockchain is the immutability also referred to as the tamper-proof ledger [26]. This helps its users to trust that the transactions are valid. Blockchain combines sequential hashing along with high-end cryptography in a decentralized system and thus makes it really challenging for anyone to tamper with the system [24]. The blockchain makes use of the consensus model protocols which means that 51% of the users in the blockchain must agree before the transaction is validated [28]. There are few companies working on extra security measures to prevent any event of 51% cyber control attacked.

Another key feature is the traceability present in the blockchain [25]. Since every transaction is digitally timestamped and signed which can lead to the exact address to identify the individual. This helps in the auditing and tracing back the frauds made by any individuals. This provides a high level of transparency in the system. Smart contracts are effective measures used by computer programs to facilitate and verify and enforce rules to be followed between parties [28, 29].

In summary, blockchain must provide Availability to complete the CIA security model. The decentralized structure model by default acts as a protection for DDOS attacks [24]. There have been several attempts of DDoS attacks over the Bitcoin network in 2014, but the Bitcoin blockchain was able to defend it successfully [28]. It has been proven to make DDOS attacks hard. However, with the increasing number of IoT devices and higher bandwidth speeds, the worst is yet to come [29].

As discussed earlier, blockchains are not vulnerable to the single point of failure which means an individual IP based DDoS attack will have no impact on the blockchain. Even if a node is taken down, data will still be available via other nodes since all the nodes always have a full copy of the ledgers [28].

5.3. Blockchain for IoT forensics

In Forensic Analysis, where establishing integrity is a crucial part to achieve the end goal, blockchain technology brings in substantial benefits [30]. Evidence collected, preserved and validated can be traced back to its original source of entry in a blockchain. This reduces the amount of time and efforts spent in investigating the evidence for its origin. Due to the increased trust consensus among the parties involved and increased transparency, transactional efficiency, and reduction in fraud is also increased. Third-party verification procedures such as due diligence, proof of ownership/title, verification of asset's existence, evidence collection etc. are also addressed by leveraging the blockchain technology features and hence avoiding the need for costly third-party involvement. With the proper adoption of blockchain technology, the implications for forensic analysis could be profound - greater transactional speeds, reduction in fraud and cost-cutting [30].

6. Conclusion and Future Research

IoT has revolutionized the world of technology and has brought tremendous benefits to human lifestyles. With all these billions of IoT devices connected around the world, it has led to a huge volume of data generated each minute; known as the "Big Data". Data has value whether it is structured, unstructured or even raw data. Various organizations are willing to pay to have these data, hence not having to invest in the IoT technologies or to monitor their competitors' data and get an upper hand. Hackers, on the other hand, will always exist and try to get unauthorized access to the data and sell it to the black market or any personal motives. There have been several security issues discussed in this review such as privacy and confidentiality. It is crucial for organizations and anyone engaging in IoT technologies to be aware of the securities issues and adopts some of the data protection. Though there are theoretical frameworks proposed by researchers for IoT security and especially in the forensics department, the challenges still exist. Since the current models do have some security vulnerabilities which might be addressed using blockchain technology features such as decentralized structure and several verification processes during the transaction. The healthy future of IoT relies on the proper security implementation.

Abbreviations

CIA	Confidentiality, Integrity, and Availability
CRM	Customer Relationship Management
DDOS	Distributed Denial of Service
DFR	Digital Forensic Readiness
DOS	Denial of Service
ERP	Enterprise resource planning
IOT	Internet of Things
MITM	Man in the Middle Attacks
PKI	Public Key

References

1. Chen, F., Deng, P.; Wan, J.; Zhang, D.; Vasilakos, A.V.; and Rong, X. (2015). Data mining for the internet of things: Literature review and challenges. *International Journal of Distributed Sensor Networks*, 11(8), 1-14.
2. Columbus, L. (2017). Roundup of internet of things forecasts and market estimates. Retrieved October 1, 2017, from https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#1a24c5161480.
3. Venčkauskas, A.; Damaševičius, R.; Jusas, V.; Toldinas, J.; Rudzika, D.; and Drėgvaitė, G. (2015). A review of cyber-crime in internet of things: technologies, investigation methods and digital forensics. *International Journal of Engineering Sciences and Research Technology*, 4(10), 460-477.
4. Khan, N.; Yaqoob, I.; Hashem, I.A.T.; Inayat, Z.; Mahmoud Ali, W.K.; Alam, M.; Shiraz, M.; and Gani, A. (2014). Big data: survey, technologies, opportunities, and challenges. *The Scientific World Journal*, Volume 2014, Article ID 712826, 18 pages.
5. Chaudhari, N.; and Srivastava, S. (2016). Big data security issues and challenges. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 60-64.
6. SAS Institute Inc. (2017) *What is big data? | SAS US*. Retrieved September 29, 2017, from https://www.sas.com/en_us/insights/big-data/what-is-big-data. html.
7. ComputeScotland (2017). IOT: What, how and where? Computescotland.com. Retrieved October 10, 2017, from https://www.comput escotland.com/iot-what-how-where-9427.php.
8. Mo, Y.; and Sinopoli, B. (2009). Secure control against replay attacks. *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 911-918.
9. Zia, T.; and Zomaya, A. (2006). Security issues in wireless sensor networks. *In Proceedings of the International Conference on Systems and Networks Communications (ICSNC'06)*, IEEE Computer Society, 40.
10. Kumar, S.A.; Vealey, T.; and Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772-5781.
11. Hossain, M.M.; Fotouhi, M.; and Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. *2015 IEEE World Congress on Services*, 21-28.
12. Gahi, Y.; Guennoun, M.; and Mouftah, H.T. (2016). Big data analytics: Security and privacy challenges. *2016 IEEE Symposium on Computers and Communication (ISCC)*, 952-957.
13. Andrea, I.; Chrysostomou, C.; and Hadjichristofi, G. (2016). Internet of things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180-187.
14. Marjani, M.; Nasaruddin, F.; Gani, A.; Karim, A.; Hashem, I.A.T.; Siddiqa, A.; and Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. *IEEE Access*, 5, 5247-5261.
15. Yu, S. (2016). Big privacy: Challenges and opportunities of privacy study in the age of big data. *IEEE Access*, 4, 2751-2763.

16. Zhang, Z.K.; Cho, M.C.Y.; Wang, C.W.; Hsu, C.W.; Chen, C.K.; and Shieh, S. (2014). IoT security: Ongoing challenges and research opportunities. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 230-234.
17. Dixit, M.; Kumar, J.; and Kumar, R. (2015). Internet of things and its challenges. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 810-814.
18. Rimavicius, M. (2015). Literature review of the internet of things: anticipating tomorrow' s challenges for privacy and security. Retrived July 29, from https:// pdfs.semanticscholar.org/2ff7/df8d97f07ebe8e04fea2ac20ac883c40a5c1.pdf.
19. Kundhavai, K.R.; and Sridevi, S. (2016). IoT and big data- the current and future technologies: A review. *International Journal of Computer Science and Mobile Computing*, 5(1), 10-14.
20. Kube, M. (2015). Six things we learned about the internet of things in 2014. Retrieved October 10, 2017, from https://blog.gemalto.com/iot/2015/01/20/ six-things-we-learned-about-the-internet-of-things-in-2014/.
21. Zawoad, S.; and Hasan, R. (2015). FAIoT: Towards building a forensics aware eco system for the internet of things. *2015 IEEE International Conference on Services Computing*, 279-284.
22. Kebande, V.R.; and Ray, I. (2016). A generic digital forensic investigation framework for internet of things (IoT). *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 356-362.
23. Meffert, C.; Clark, D.; Baggili, I.; and Breitinger, F. (2017). Forensic state acquisition from internet of things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17)*, ACM, 56, 1-11.
24. Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, 19(4), 68-72.
25. Cai, Y.; and Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation*, 2:20, 1-10.
26. Pierro, M. Di. (2017). What is the blockchain? *Computing in Science and Engineering*, 19(5), 92-95. Retrieved September 29, 2017, from http://ieeex plore.ieee.org/document/8024092/.
27. Teslios, C.; Politis, I.; and Kotsopoulos, S. (2017). Enhancing SDN Security for IoT-related deployments through blockchain. *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN).*
28. Piscini, E.; Dalton, D.; and Kehoe, L. (2017). Blockchain and cyber security. Let's Discuss. Retrieved November 29, 2017, from https://www2.deloitte. com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandC yberPOV_0417.pdf.
29. Puthal, D.; Malik, N.; Mohanty.; S.; Kougianos, E.; and Yang, C. (2014). The blockchain as a decentralized security framework. future directions. *IEEE Consumer Electronics Magazine*, 7(2), 17-19.
30. Lee, J. (2018). Beyond bitcoin: Leveraging blockchain for forensic applications. *Grant Thornton.* Retrieved September 29, 2017, from https:// www.grantthornton.com/library/articles/advisory/2017/leveraging-blockchain -forensic-applications.aspx