Published in AJSE, Vol:20, Issue: 2
Received on 10th October 2020
Revised on 1st March 2021
Accepted on 30th April 2021

AIUB JOURNAL OF SCIENCE AND ENGINEERING
ISSN: 1608 – 3679 (print) 2520 – 4890 (Online)

Investigation of Security Challenges from the Perspective of Stakeholders in IoT

Md Sajid Bin Faisal, Ahsan Habib, Md. Aolad Hossain Anna, Cynthia Rashid Simin, Dip Nandi

***Abstract: Internet of Things (*IoT) has become one of the major study concerns and prospects in recent times. The ecosystem that makes the interconnection between person, objects, device in a secured acceptable and useful manner is in the boundary of Internet of Things. One of the major concerns in IoT is its security and the technologies which are working behind. The security measures are taken under a vast amount of studies and applications. The concept of this research is to consider the existing technologies that are working for security assurance and the challenges which are faced by different angles of participants and manufacturers due to make IoT a secure electronic ecosystem. Basically, the focus over the security challenges are on the stakeholders and they are user, manufacturer and service provider. At last in this literature, the security-oriented level of challenges (integration, costing, handling & observation) have been mathematically produced from the 3 different perspectives of the stakeholders mentioned.**

Indes Terms*— *prospects, Ecosystem, participants, platforms, manufacturer, applications, considerations, stakeholders

I. INTRODUCTION

The Internet of Things has become one of the mostly debatable and concerning topic in the present world. The current information and technology industries are trying to make the circle of IoT's diameter longer as much as possible. As IoT deals with customers, service providers and the manufacturers, a major concerning and mostly wanted area is its security. Also, challenges are being faced for ensuring the security in this sort of global and wide range of interconnected Cyber-physical system.

Md Sajid Bin Faisal
Student, MScCS
American International University Bangladesh (AIUB)
Email: sajidfaisal80@gmail.com

Ahsan Habib
American International University Bangladesh (AIUB)
Email: ahsanpolok156633@gmail.com

Md. Aolad Hossain Anna
American International University Bangladesh (AIUB)
Email: aolad.anna@gmail.com

Cynthia Rashid Simin
American International University Bangladesh (AIUB)
Email: cynthiasimin91@gmail.com

Dip Nandi
Associate Professor and Director, Faculty of Science and Technology
American International University Bangladesh (AIUB)
Email: dip.nandi@aiub.edu

The technologies which are being used and existing in current industry visions are being analyzed one by one in the review. The block chain, AES cryptographic standard, Wireless Sensor network, Radio Frequency Identification, Key management, Cloud computing and Architecture of IoT has been analyzed and briefed theoretically for better understanding. According to the analysis and the basis of the literature description, the security ensuring challenges are being faced from the 3 angles or view points of the people whom are connected to IoT. As we all Know IoT is the place where human, things and smart objects are going to be taken together or tied up. IoT is basically the intelligent environment around us with the help of Wireless Sensor Network and the vision of the future internet from Mark Weiser [1]. Later the concept had been through evolutions from Kevin Ashton to the current concern of "Users Privacy and threat Management". A proposal of the security challenge from various perspectives of IoT has been scaled by levels in this research.

In our literature review-based research, we have analyzed and discussed over the technologies followed by the state of research on security challenge domain in table I. Also, we tried to present the sequential concept of the research work flow by a Pyramid in figure 2. A cloud system based IoT's visual representation had been shown in figure 1. Then, the challenges were analyzed in table II that showed the 7 x 3 matrix of challenge level from 3 different observations of the stakeholders. Later on, the whole process had been discussed about the future working sectors and possibilities of advanced research on the same problem. However, the major contribution of this article is that it provides a security centered challenges faced by the 3 types of stakeholders to obtain and analyze which is shown at table (II). The focus has been the level of faced challenges for each of the technologies for the discussed stakeholders.

II. IOT BACKGROUND

The number of devices getting connected to wire or wireless based internet service is increasing day by which will provide powerful source of information to us. IoT is such thing that converge data of different source to any virtual platform on existing internet infrastructure. IoT basically allow autonomous exchange of important information between invisibly connected real world devices which fueled by the leading technologies like Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) and sensed by the sensor devices following further processed for decision making. To conclude, IoT creates an environment where things can talk and their data is used to perform targeted tasks through machine learning [2].

The IoT involves billions of different devices inter-connected by 2020 huge amounts of rapidly growing data ("i.e., "big data"), and so many devices. Sensors, actuators, smart phones, computers, buildings and home/work appliances, cars and road infrastructure elements are the devices [3]. The Internet of Things is there to make lives of millions easier as the day progresses and the technology gets more and more advanced. IoT has brought the things, objects interconnection that also

involves the people in it. The modern-day enterprises and services are being developed and provided by the Internet of Things. It may include the presence of more than 200 million devices by the end of 2020. It is creating a huge collaboration of the people and its services as the technology advances forward [4]. IoT works with a variety of research concerns. Especially, the connectivity and network upgradation is always required for a better experience. For better coverage Wi-Fi, WiMAX Bluetooth, router and wireless network services has become essential. The devices that are capable of being connected with the Wi-Fi and wireless technology is increasing its demand day by day and the manufacturers of these are always keeping in mind about their network assignment and covering capabilities. Different types of devices are being interconnected for the sake of data transmission and processing in between the objects in IoT [5]. The concern is to make a lightweight and less energy consuming secured architecture that requires to be in the IoT model of research. That architecture may be able to work with existing world of sensors and technologies within a secured and less vulnerable environment. This must be considering the IoT based applications and localization, routing protocols and expandability in heterogeneous environment and node tracking in Wireless Sensor Networks [6]. Wireless Sensor Network (WSN) is the sensor dependent network structure that suits the Internet of Things concept. The interconnection of the computational standard and process arena must be linked with the physical systems, devices and object. WAS based network is based on the addition of multiple number of wireless sensor networks on the internet that has the access of the specific database and web servers. The main goal of these networks is to reduce cost, being capable of heterogeneous network and platform. The data is passed on the databases by counter number of request generation from the gateway to the webserver [7]. Basically, the concept is to provide the ecosystem of wireless sensor networks, home office appliances and objects with proper network gateways. In the world Internet of Things security and privacy is a major issue that can never be neglected. So, for the interconnected objects and devices should be able to authenticate themselves within the network. The WSN, RFID sensors, cloud computing and low power networks are there to provide the facilities of being interconnected in various manners like distributed, centralized, decentralized, collaborative manner. In terms of making the IoT system more reliable it must be ensured that the system produces satisfactory level of security. Mainly, user and object verification, authentication, access control, confidentiality of data, trust issues, network layer security, entity relationship and information dependability with mutual understanding among them are considered as challenges for IoT security [8].

A. Problem Statement

It is clearly seen that the previous researches have mentioned about the security challenges and its process of management in IoT. Having considering the security challenges of the previous literatures of the authors mentioned, there were no sign of stakeholder-oriented security challenge level definition to separate the faced challenges in IoT regarding security. This literature study aims to focus on the problem which is based on the stakeholders' vision. The security challenges are leveled into a certain range to show which of the technologies are more challenging to maintain for what sort of stakeholder. In the end, this article provides an indication to the challenges faced by the stakeholders' which the previous literatures lacked to focus on. None of the researches were found to deal with the stakeholder's challenge level in terms of security which this literature tries to produce in the end.

TABLE I. Legacy of Research on Security Challenges

Sl no	Author(s) name	Name of Article	Publish year	Concept of work
1.	Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh	IoT Security: Ongoing Challenges and Research Opportunities	2014, November	The discussion over the security related issues and challenges over a number of topics. The challenges which included here were Identification and locating, lightweight cryptographic system, ongoing research sides as the challenges in Software vulnerabilities, Authentication and Authorization, Malware control and Privacy were the topics. Also, the domain naming system and the overheads occur in Lightweight cryptosystem is a challenge. The analysis of the various sides of Android architecture and its feature-based challenges and issues [9].
2.	Rajendra Billure, Varun M Tayur, Mahesh V	Internet of Things - A Study on the Security Challenges	2015, June	In this Article the identification of Securing IoT environment, current state of IoT security by examining the literature and research challenges. They also discussed about the interconnection of the devices that helps improving both automation and augmentations. It was focused in the communications occurring on the public network that mostly need to be secure path when data is exchanged. They have also found some security challenges, middleware

				components and recent developments in their lecture review [10].
3.	Ibrar Yaqoob, Ejaz Ahmed, Muhammad Habib-ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-Garadi, Muhammad Imran (IEEE member), Mohsen Guizani (fellow)	The rise of ransomware and emerging security challenges in the Internet of Things	2017	In this article the security concerns in an IoT system is described along with the necessary and smart IoT includable applications. The Ransomware is a form of malware that denies access of the real owner by encrypting files. The challenges in IoT arena and the present notable threats are discussed in the article. Most importantly it provided the taxonomy of IoT security divided in 5 parts. They are classified as: Threats, Requirements, Deployment, Technologies and IEEE Standards [11].
4.	Tariq Aziz Rao, Ehsan-ul-Haq	Security Challenges Facing IoT Layers and its Protective Measures	2018	Usually, the regular network comprising upon a personal computer, servers and smart-phone whose resources are adequate, whereas, IoT system is composed of RFID and WSN nodes whose resources are inadequate. This article concerns about the security challenges facing four fundamental layers of IoT (Perception Layer, Network Layer, Processing Layer and Application Layer), different types of attacks on these layers with instances and point out the privacy measures to increase the robustness and authenticity of the IoT. This paper will be supportive for the IoT applications' developers from the security perspective as well as the researchers [12].
5.	Sha, Kewei, Wei Wei, T. Andrew Yang, Zhiwei Wang, and Weisong Shi	On security challenges and open issues in Internet of Things	2018	In this paper, an IoT architecture of 4 different layers (Application, Cloud Edge & Things) are shown. Resource constraints, privacy, integration with the current technology and a recent overview of security are analyzed. A brief comparison between IoT and the WSN technology focusing on their Privacy, Heterogeneity, Communications and Scalability & Coupling is produced. Architectural security design for end-to-end, edge layer and distributed security design is provided visually with discussion [13].
6.	Mauro Conti, Ali Dehghantanha, Katrin Franke, Steve Watson	Internet of Things Security and Forensics: Challenges and Opportunities	2018	This paper is distributed into 3 major sections in IoT security. At first the focus was over the Security Challenges in IoT concerning the Privacy, Authentication, Access controlling and management of access & Secure Architecture on Software Defined Networks and Cloud Infrastructure. Next the IoT environmental forensics and issues have been listed and demonstrated according to the upcoming and present scenario of IoT. The matters like Identity collection, correlation, Evidence, analysis and investigation with the probable attacks malicious act have been identified. At last the issued & selected papers of the 3 major domains of security, privacy & SDN system is listed with identification and review [14].

As security being one of the major considerations in terms of any application to be included in IoT, the systems, applications and objects which contradicts the idea of security assurance in the system may not be accepted for long term usage. There is various network layer-based architecture, asymmetric key cryptography, security protocols for lightweight systems are helping day by day to strengthen the security standards in IoT. All of them focus on the edge, cloud and things layer of the IoT system. These three layers in combination creates the basic architecture of secured IoT system. The things layer concerns about the physical world, software and sensor technology's strong bonding, where the cloud layer is actually working as the larger storage that is far away from the devices. And these devices needed to be bonded between themselves even if one of them is low power and the other is a high-power cloud-based system that has got lots of tasks to accomplish. These different types of powered devices are bonded in the edge layer [15]. So, it goes without saying that security architecture based IoT standard is a matter of study for the recent growth in the industry. There are several issues and security related challenges which is faced in IoT for

about 15 or more years. The paper is going to consider most of them including RFID, WSN, authentication and asymmetric key management, Block chain and cryptanalysis, AES, Cloud storage and computing. The first among these and the one that started off the conception of IoT is RFID back in 1999 [16]. Kevin Ashton was the man who first used the Phrase "Internet of Things". The embedded system within the internet had been evolved to today's form since then. Wireless Sensor Network is also a base on the Internet of Things and its connectivity. Block chain is a very useful concept for security. The chain or legacy of nodes are being used for decentralization, security and scalability. Takoshi Nakamoto came up with the plan of bitcoin. The bitcoin or cryptocurrency was first applied by the help pf block chain. The nodes in the chain are there for receiving and storing data and cryptographic technique is used for the form of cryptocurrency and peer to peer transaction. Also, it is used in Ethereum that are contracts the user can trust on for storing, messaging and acting on behalf of the user on a contractual basis [17]. Basically, the target of this research is to establish a level of challenge from the user, manufacturer and the service providers' perspective.

III. NECESSITY OF SECURED SERVICE PLATFORM

Securing IoT devices is a real challenge now a days. Security is necessary in IoT because we share/communicate with other devices using IoT. We also store Personal Data which is at high risk if it has been hacked. Also, for every industry IoT is important and they definitely make use of it for sharing the data, tracking live location and more. If all this data is misused it can affect the businesses overall, thus security is important in IoT.

There are two key issues privacy and security that need attention when it comes to IoT security. From corporate servers to cloud storage, cybercriminals can find a way to exploit information at many points within an IoT ecosystem [18]. However, securing IoT systems is also more challenging because of characteristics of IoT systems, including extremely large scale, low cost design, resource constraints, device heterogeneity, preference of functions over security, higher privacy requirements, and harder trust management.

IoT security has been introduced to the industry and is used in various ways:

- Cyber-Physical Systems (CPS)
- Cyber Transportation Systems (CTS)
- Machine-to-Machine(M2M) Interaction

IV. ANALYSIS OF EXISTING TECHNOLOGIES

The frontline technologies are described according to IoT scenario and service scheme. The background analysis of the technologies is needed before getting into the focused work.

A. Radio Frequency Identification (RFID)

Radio Frequency Identification is a vastly used technology in IoT arena from the very beginning. The technology basically works through the radio frequency channel-based assignment of people, things, machine and computers through sensors. The two major components of the RFID are the readers and the tags. Actually, readers are the receivers and tags are considered to be the transponders. RFID is the link between the virtual and outside world of things. The data needs to captured from the real world and processed into the virtual world in order to transmit into the destination receiver. So understandably, it has to deal with perception layer, network layer and service layer. The perception layer receives data by the user through various technologies like tag reader, writer, GPS, WSN etc. The transportation process of the data is done on the network layer via microwave and other existing wireless communication and data transmission technologies. The last layer is the service/application layer that enables the RFID system into the data passage and transmission to the destination. RFID data flow means the "command" and "responses" directions among the application, reader and tag. RFID tags works as the data transfer and readers are used for receiving purpose. There are various classifications of the RFID devices that are labeled from level 0-5 depending and classified on the basis of Radio frequency passage, programmability, memory capability, battery and power consumption, communication standard and efficiency of process [19]. This system is used in medical sciences, military, industrial works, transportation, banking, agriculture fields etc. RFID pin distribution, cloning, authentication and hash lock up, Elliptic curve cryptography and security requirement and identification is described in "Communication Protocol of RFID Systems of Internet of Things" from CS department of Central China Normal University. A proposal of SPAP and random Oracle model is defined and constructed for RFID [20] in the mentioned paper. The working process of EPC tags, RFID middleware and mathematical usage of symbols and security requirement model is briefly described with proper Tag and Reader based technology.

B. Block Chain

The internet services have gone towards the use of block chain after the evolution of the Block Chain Cryptanalysis for node to node successful transaction. The bitcoin is a cryptocurrency system that has created the demand of Block Chain concept in the modern world. The Block chain usually works by the critical mining process run by the PoW (Proof of Work). This basically creates an overhead to the system along with notable amount of energy consumption. It can create the interconnection of a certain decentralized and distributed scalable service platform or network. Each block carries internal storage, transaction information and hash value from previous block. Also, the Merkel Root is the hash value of the present block. A specific time stamp or time limitation is set for the miners required to take for the mining process. That is called the "Consensus" process [21]. Block chain is gaining much attention on various industries communication and transaction process. The system is now one of the leading computers system-based protocol that is being followed. The block chain enables the use of multiple nodes or blocks in a chained order from ancestor to successor. The internal transactions and computations are done by the mining process of the nodes. The blocks contain the hash value for the parent, their own "nonce" value for hashing and the time stamp for transaction process. The acceptance of the Block Chain is increasing rapidly among the commerce banks and legal regulatory organizations [22].

The miners need to be very much active on the success of mining. Securing the nodes in the chain is the key concern of protecting the data inside the chains. The mining power may lead to the ability to get in the charge of the block chain. Forking problems are also faced in the chains between the older and new nodes in the chain. Proof of stake does not require electrical power to run the mining process. PoS reduces the probability of attacks in the chain. Though having some limitation over PoW, PoS provides low power consuming mining standard. Also, it draws a line between the stakeholders and the miners in a certain market place [23]. Also, the Block Chain concept supports the ability of the distributed design of the specific system with convincing scalability that helps in transactions, though the security ensuring standards on BC remains still in research.

C. Advanced Encryption Standard (AES)

A 56 bit of encryption standard Prepared for gaining a cipher text by the help of a number of lookup tables in a round. The DES algorithm had been broken by the attackers in a very short period of time that is within a day. So, the necessity of a stronger encryption algorithm with greater complexity and mathematical approaches felt by the researchers [24]. Such algorithm needed be built by a round of mathematical calculations, permutations and combinations rather than going for some look-up tables and get the corresponding data. The name of the algorithm had been previously used as RIJNDAEL which was later considered as the AES. The name of the mathematicians were John Daemon and Vincent Rijmen. The name of the standard had been firstly made with the last names of these two gentlemen [25]. The AES encryption comes along with 3 different types of cipher key length of 128,192 and 256 bits. It is internally consisting of 4 types of mathematical changes in each round. The MixColumns step is only executed during the last cycle of encryption. The Process starts with a cipher master key generation that is X-ored for getting the AddRoundkey during the start of the operation and changing its state array of 16 bytes for AES 128 standard. Here each byte can be considered as a single block also [26]. The operations are done for each round from AddRoundkey to ShiftRows.

AddRoundkey: A 16 block key is generated and that is x-ORed with the 16-block corresponding state array. Thus, the round key of 16 bytes is obtained.

SubBytes: This is done by two different processes. The generation of S-Box lookup table and the byte inversion from Galois Field (GF 2^8) =256 number of entries with affine transformation from the table values. The corresponding changed state array of 4 x 4 blocks goes to the next operation.

ShiftRows: This process makes the circular left shift of a certain row according to its value of row. There will be no change in the first row. The second third and fourth row circular left shifts 1, 2, 3 blocks respectively in a circular manner.

MixColumns: This is only performed at the last round of cipher algorithm [27]. The columns are likely to be multiplied with a certain function of size 4 x 1. Thus, the state array is changed after the multiplication.

Basically, AES is a lightweight symmetric encryption standard.

D. Authentication & Key Management

In an IoT environment it is always a stressful task to authenticate the user and controlling the access of specific users in a network. Also, we use different cryptographic methods for encryption. So, key generation plays a vital role in the encryption system. As a result, managing the key is a concern as well as these keys can cause a large overhead into the system and the performance of the running process. So, it is challenging to maintain and manage key in these encryption and authentication systems. That is why private information securing and maintaining its access controllability is also a challenge in the manufacturer perspectives. The quick identification of the part or node in the network that actually is gathering and leaking information is needed to be done by the authority or service providing sides. From which nodes the information is being leaked that may also be identified [28].

Basically, intruder detection and noticing them in the network is a concern in security. It should be detected that from where the malicious and harmful tasks are being accomplished in the network. Smart medical assistants that can carry the health-related data about health of individual users are personal data in IoT. Blood pressure, glucose level measurement, medical assistant, emergency health service, connection of the related medical devices and rehabilitation center are the technologies which are being used in IoT based medical services. For using these services, the trust gaining of the users is a must. So, a strong cryptography is necessary such as AES, RSA and DES. Rivest-Shamir-Adleman (RSA) is known as an asymmetric cryptographic technique that is much secure compared to another symmetric cryptographic Standards AES and DES. RSA algorithm is well known for its two different keys public and private key of encryption.

The process involves the multiplication of two random numbers ‘r’ and ‘s’ that needed to be 1 less from their value each and then multiplied. By that value of second multiplication, we get the first value of our public key. Actually, we have found the value of integer d (assume) that d.e mod (p-1)*(q1) =1. Here the public key set is (e,n) and the private key set is (d,n). Where n is the multiplication of r and s. That is how the public and private keys are generated.

Assume message is ‘m’ then,

eq1: m^e mod n (this is for getting cipher text)

eq2: (cipher text)^d mod n (this is for getting plaintext back)

This is how this RSA asymmetric cryptography works for securing data by key generation [29].

E. Cloud Infrastructure

Cloud based storages immensely altered the concepts of resource-based Computing. People are using cloud storage for storing and to Share data. Security is a concern but users are not aware of those security issues. People of all over the world are using it and sharing data. Cloud transmits personal sensitive data [30]. Cloud environment related with virtual and physical resources and shows different type of security issues and fully addressed threats of existing problems. Cloud accessed account contains security issue that leads to data loss. Developed internet technology can handle those issues. Consumers are not able to know the risk in the cloud transaction [31]. Cloud computing

comes with different number of challenges and security critical barrier and numerous possible challenges and also, Dynamic and vast security challenges in cloud computing. This is not an easy task for us to secure big data and computer networks [32]. When we are logging in different location and servers the security issues are arise for cloud computing. Also, when we use shared cloud for any purpose that is even more challenging for us to secure the data and the data location is also a critical factor for securing cloud [33].

Cloud security ensures policies of high rate significance with customers both personal and business. Personal data security is a big concern in Cloud and IoT. Many of the big organizations are not interested about cloud server without security justification [34]. Security is a main part of a cloud server and also for earning trust. It should be kept in mind, trusting someone may also arise security issues [35]. It should not be forgotten that, all kinds of attack is possible in computer network. DDoS, phasing, middle man attack. For Attacking of cloud server, it concerns data loss or leakage. DNS poisoning is big risk of whole computer network including cloud. Well known encryption method can protect those kinds of attack or new invention of encryption-based algorithm can gain trust of people who are using cloud computing and storage [36]. Using of third-party API is also harmful in cloud. Paid APIs can solve those security issues. Also challenging for software bugs, human errors is the cause of weak security. Debugging those kinds of issue may make a handy experience of the users. User friendly software is more effective [37]. Session and cookie are the main part of any web-based site. Session work in the part of server site and cookie work in the part of browser and also perform at server site. Session hijacking is one of the potential security threats. Same things are happening in mobile cloud storage [38].

User friendly interface can change the experience of users of cloud computing and user can get easily habitant with it. Users can utilize the encrypted data. Virtualization is a technology that connects with cloud computing. There are three ways where physical platform deliver the number of users can get in, those are SaaS, PaaS and IaaS [39] [40].

The cloud services are that working in IoT Platform needs be capable of being matched with the heterogeneous network environment. The data files must be converted to an enlisting and descriptive annotated form of data in the data link layer. Then it can be easily added to the Applications, services and Linked data sources in Internet. It may try to cover up all the possible services in a platform with all the necessary applications by data linking [41]. Here shown the visual representation of what the things and services need to be there in the Internet of Things perspective for service oriented applications in future.

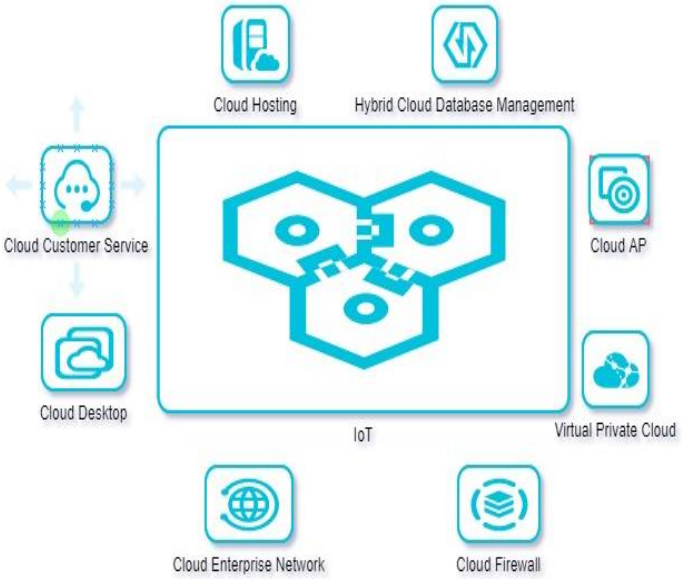

Fig. 1 . Cloud Based IoT system's visual representation.

F. Wireless Sensor Network (WSN)

The IoT system of the Physical elements is composed in Perception layer. In IoT Fundamental issues for IoT solutions is data confidentiality that is particularly relevant in the business context. Current data confidentiality is not solved because of two main limitations those are the amount of data generated and the Effectiveness of control assess data.

A group of independent nodes are wirelessly communicating with limited frequency and bandwidth is defined as WSN. The main limitations of wireless sensor network that is network discovery, power management, routing, control, collaborative signal and information processing, security, tasking and queering. These following components are including in WSN networks that is Hardware, Communication stack, Middleware, Secure data aggregation. Similarly, Radio Frequency Identification (RFID) collects some data by sensor for purpose of analysis in the centralized the systems [42]. Theoretical and practical visions and concepts of IoT security which take into account end-node resource limitations, communication protocols, applications characteristics and IoT hybrid network architecture. A series of potential DDoS attacks to infect a large number of Internet-connected devices, hit several companies with malware attack in September 2016. The devices got out of date on their LINUX. These may be the reason why they were attacked by DDoS [43].

Necessity of WSN in IoT:

Internet of things is often considered as the service of wireless interconnected devices. The services are expected to be wireless and uninterrupted from the user's point of view. Most of the modern services, tools and machines are deeply dependent over the structure of a powerful and authenticated wireless network. Wireless networks do the activity of a widespread distanced network of the system. It allows the users of diversified networks to be enlisted within a single wireless network. A group of sensors are classified according to their tasks and thus it creates an architecture. One of the major reasons of the emphasis and attention for the WSN networks is it is less collision prone [44].

The transmission time collision is always a problem for any network architecture. Thus, the usage and popularity of wireless sensor network over any other network structure increased. The data passage through the sensors to the centralized processor on the internet enables the processing to be more problem free and precisely generated. Nevertheless, the energy efficiency of the WSN technology is often considered satisfactory as per the expectations. It is only possible due to multi hopping technology of wireless networks. As the group of sensors work as the different heads of cluster, it is easier for a transmission to traverse from node to node. Also, the distance between the sensor's nodes are minimal, so the transmission energy is minimal. This is how it is clearly considered that it is more energy efficient compared to single linkups of radio signal coverage. Finally, the widespread use of the WSN network has increased in the internet of things in recent times.

G. Architecture & System Protocol

Digital communication which was defined a long time ago for a key role to the TCP/IP protocol stack. IoT connects a number of objects enormously which create traffic and a huge amount of data capacity. IoT needs to address many essential factors that are being faced in managing the networks and the services. They are demonstrated below:

Sustainability: The service should have a certain level of tolerance of errors and problems in it.

Reliability: Must gain the trust and respect from the users. The users should be flexible in depending on the services and its issues.

Quality of Service: The Quality is the greater concern than any other in a service. So, the quality must not be neglected by the service providers.

Confidentiality**:** The data is maintained by the governing service providers in IoT. Confidentiality should be kept by user's data access and prevention from sharing with unwanted people, objects.

Integrity**:** During the communication process is being executed, the change or manipulation of a single data is strictly restricted. These are the things to look up, for the new standard architecture and protocols. There should be a well-accepted protocol that actually capable of solving the existing concerns and issues in security for the IoT networks. IoT receives data via smart sensors then transmits the data to the processing system using an M2M (Machine to Machine) device. The typical architecture of IoT is getting data from outside by some perception sensors or devices are mostly deployed due to the absence of monitoring systems, these create vulnerabilities and lead to the attack from the outsiders. An attacker can continuously send data to potential network intruders [45].

V. METHODOLOGY

The identified findings of the security challenges in IoT along with proper background knowledge and evidence is followed by the challenges faced from various perspective in a particular system. The basic problems and challenge detection is demonstrated with a Table (II) with justified literature observation. So, this can be considered as a descriptive research with qualitative approach. The key concern of this study is stated below:

Can we define/construct a security level matrix of challenges from the different point of view of the stakeholders?

The existing technology needs to be addressed first and then the challenges which are recently being faced and not properly solved. Therefore, the maintenance of these technology can turn to a hazard and matter of challenge. The next discussions are focused on the angles of the challenges.

Conceptual Pyramid structure of the Research:

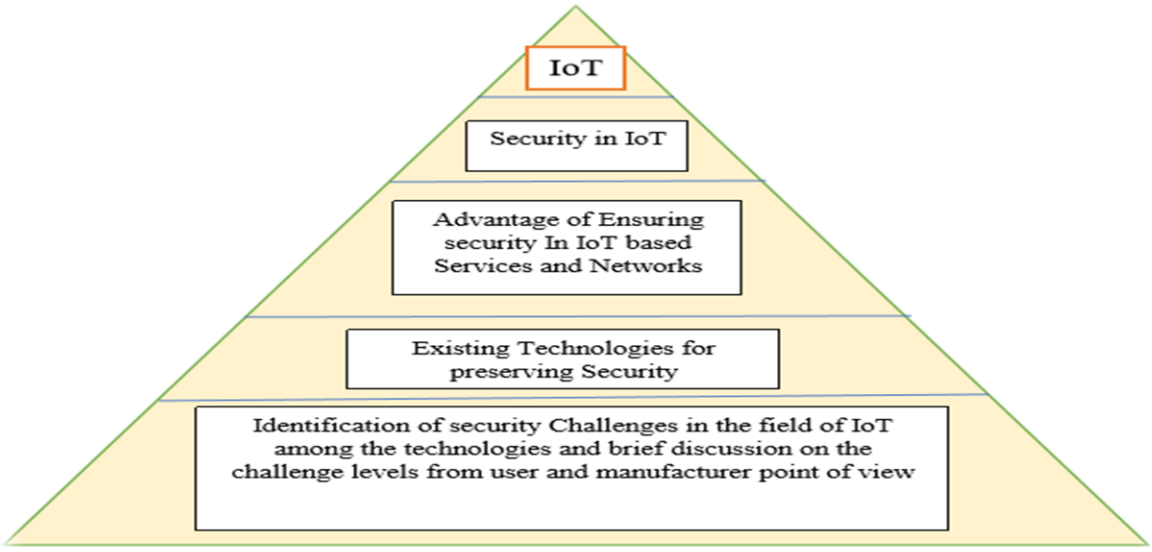

Fig. 2. The structure (pyramid) of the research work plan

Process of Calculation:

The process of calculating the matrix of security challenge may not be accurate but informative and justified by the literature evidence and their legacy of challenges. Suppose, if a security-based challenge affects or hamper one angle; such as user, the user is noted as one "1". If it does not put the manufacturer and the service providers into a challenge then they can be entered "0" in the table. In this manner if the challenge is faced by the particular angle and they are affected by the judgement of the current situation, they are noted "1" and "0" if not. In the end all of the particular criteria of security challenges "1"s are added from each angle and then divided by 3 to get the approximate average assumption form 3 angles as a whole for the particular technology. If the average assumption or approximate neat measure is a fraction then, if it passes the half of its fraction to the next positive integer then it is ceilinged. The value is floored otherwise. The scale of challenge level is held maximum of 3. So, if one technologies' security challenge exceeds 3, then they are considered or assigned 3 as per the scales limit. The number of challenges faced by the 3 stakeholder's numbers are basically summed for each of the technology described in every row for table (II). Then the summation in each row / technology is divided by 3, changing the fraction reading to either floor or ceiling the value for relative approximation and differentiating numerically.

This is how the table in Table (II) is constructed. The proposed matrix of level detection is done under the basis of IoT current issues, problems, considerations, acceptances, calculations from different view. Here, the Scale of (0-3) of challenge level is assigned according to the concerns, challenges, tasks to accomplish and solution opportunities of the Stakeholders respectively.

TABLE II. Security Challenge Matrix for Stakeholders (7 x 3)

SL	Usable technology in Security	Challenge(s)	USER VIEW	MANUFACTURER VIEW	SERVICE PROVIDER VIEW	NEAT CHALLENGE LEVEL
1	RFID	High throughput in Identification; huge data management; channel assignment and collision detection; IPv6 address space required [46]; Less computational ability [47]; No accepted protocol in WSN [14].	0 + 0 + 0 + 0 + 1 + 0	1 + 1 + 1 + 1 +1 +1	1 + 1 + 1 +1 + 0 + 0	(1+6+4)/3 = 11/3= 3.67 or 3
2	Block Chain	Attacker can get full authorization of the chain having at least 51% of the nodes and can deteriorate service or halt [48]; PoW mining gets difficult as number of hashes increases reducing the success probability of errorless mining which leads to errors in Consensus [49,50,51]; Still a demand of acceptance for a network architecture that works best on BC [52].	0+0+0	1 + 1 +1	1+0+1	(0+3+2)/3 =5/3=1.67 ≈2
3	AES encryption	Not concerned with the end devices encryption power [53]; must maintain the Single key efficiently and secretly by changing them frequently within few days [54].	1+0	1+1	0+1	(1+2+1)/3 =4/3 =1.33≈1
4	Authentication , key management and RSA	Efficient Key management and exchanging key causing overhead; access control and authorization in heterogeneous network [20].	0+ 0	1+1	0+1	(0+2+1)/3= 3/3 ≈1
5	Cloud Storage	Gap identification in Security [55]; accomplishing data logging in several servers and location with	0+1+1 +0	1+1+1+1	1+0+1+1	(2+4+3)/3=9/3 ≈3

		no direct connection with storage to end device [56,57]; For sudden DDoS attack, companies maintain internal bandwidth which exceeds provider supplied bandwidth [58]; Data transfer mode, broadcast nature [59] .				
6	WSN	Large volume data causes network traffic; Existing schemes are not best suit for WSN [60]; False routing among wrong nodes causes service interference; The hop to hop routing leads to transmission delay, drop and misleading interconnection among nodes [60]; availability of node's power for connectivity when required [61].	0+0+1 +0+1	1+1+0+1+0	0+1+1+1+1	(2+3+4)/3 =9/3≈3
7	Architecture Based	Dealing with software-maintained networks and cloud infrastructure [62]; Attacks and dilemmas in long distance communication of end devices [54].	0+1	1+1	1+1	(1+2+2)/3 =5/3 =1.67 ≈2

VI. DISCUSSION

The study is based on the security on the various sorts of Stakeholders who are using, manufacturing and providing the services of an IoT ecosystem. Each and every service of IoT focuses on the privacy, security, authorization, access control, scalability, communication and architecture. Also, the service needs to be deployed in a manner that ensures the security and able to get rid of the security related challenges in it to gain dependency. The work is actually based on the literature and background description of the 7 existing and frontline technologies. At first the description of the security and its necessity is given along with the proper analysis of the 7 technologies. These technologies were selected upon the currently used systems and the challenges that are mostly faced on these. The justification of the paper and citation selection were done in the same approach of the recent scenario, security scheme and amount of use in the deployed environment. So, the challenges were analyzed upon the views and role of a specific stakeholder under certain technology by mathematical condition and summation. And thus it was leveled up to 0-3 considering each of the 3 views of Stakeholder.

The reason which makes this study quite different from the other ones in Table (I) that have been researching on the same topic of security challenges of IoT is that it provides a level of challenge and precedence for each of the stakeholders who faces the challenges of the technologies considering security aspects. Also, it is the work that enables a view from 3 different stakeholder's angle in a service of IoT that helps each of them to understand and troubleshoot or solve their particular role. That may help the IoT service platform more organized, reliable, responsive and trustworthy. The work is basically based on the challenges level in terms of security aspects in Internet of things. Hence, only the challenges are enlisted by their levels from various perspectives, yet no such solution scheme. The found data are basically gathered from various articles and papers and the understanding is acquired from analyzing them in various scenarios. The technologies mentioned here are not all the existing ones yet, they are the front-line systems in IoT. Also, the frontline technologies' leading and mostly faced security challenges are shown briefly as much as possible. There can be some more group or bunch of people in IoT other than these three taken into consideration. The work is a reflection of a Current Security – Challenge vision in IoT.

This matrix presentation of challenges for the existing technologies from various perspective of people in IoT should help to analyze and enhance the identification procedure of challenge finding. Yet the software development based IoT may get help from this sort of level assignment for the current technologies. As the development and security centered challenges are basically classified by [63]:

1. Organizational: The structure of organizational protocol that ensures the security and avoid the birth of any new challenges in the IoT system.
2. Technological: The identification of the technical solutions and the ways to take the countermeasures in the development of the future versions of a service and the maintenance protocol.
3. Methodological: The concerning criteria is to find out the ways of challenge elimination and create new ways of research possibilities in the security point of view.

VII. CONCLUSION

The technique which is followed here is the frontline technology overview and background analysis which help to construct the table in Table (II). The scale is held up to the limit of 0-3 because, it is enough for showing the difference of levels. Therefore, the analysis was based on background knowledge, recent situation and simple mathematical process. This research may help the researchers who are working on the general framework and the current challenging tasks to accomplish for ensuring security. It may help to increase the security standards and protocol in IoT. The concerning nodes in IoT which should be considered in security are the People, Process, System. The interrelated objects that creates the challenges to the other 3 are surrounding it [13]. So, this level assignment of the security challenges for people based IoT ecosystem may help the researches in security domain and contribute to the service upgradation in the future. The state of research and concepts of the articles on the security challenges of IoT has been given since the year 2014 to recent time. We have analyzed a discussion on the security challenge matrix that can guide in security assurance and problem Identification in IoT. This work can guide the developers and the manufactures to focus on the technologies that are of higher priority in terms of security maintenance. Because of shortage of resource and schedule, we could not automate the challenges faced by the stakeholders. In future, this matrix can be analyzed with more dimensions of consideration to improve the concept of security related challenges.

REFERENCES

[1] Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): definitions, challenges and recent research directions. International Journal of Computer Applications, 128(1), 37-47.

[2] Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things

[3] Biswas, A. R., & Giaffreda, R. (2014, March). IoT and cloud convergence: Opportunities and challenges. In 2014 IEEE World Forum on Internet of Things (WF-IoT) (pp. 375-376). IEEE.

[4] Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. International journal of communication systems, 25(9), 1101.

[5] Talwana, J. C., & Hua, H. J. (2016, December). Smart world of internet of things (IoT) and its security concerns. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 240-245). IEEE.

[6] Wang, C., Daneshmand, M., Dohler, M., Mao, X., Hu, R. Q., & Wang, H. (2013). Guest Editorial-Special issue on internet of things (IoT): Architecture, protocols and services. IEEE Sensors Journal, 13(10), 3505-3510.

[7] Kuo, Y. W., Li, C. L., Jhang, J. H., & Lin, S. (2018). Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications. IEEE Sensors Journal, 18(12), 5187-5197.

[8] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

[9] Zhang, Zhi-Kai, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. "IoT security: ongoing challenges and research opportunities." In 2014 IEEE 7th international conference on service-oriented computing and applications, pp. 230-234. IEEE, 2014.

[10] Billure, R., Tayur, V. M., & Mahesh, V. (2015, June). Internet of Things-a study on the security challenges. In 2015 IEEE International Advance Computing Conference (IACC) (pp. 247-252). IEEE.

[11] Yaqoob, Ibrar, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, and Mohsen Guizani. "The rise of ransomware and emerging security challenges in the Internet of Things." Computer Networks 129 (2017): 444-458.

[12] Rao, T. A., & Haq, E. U. (2018). Security challenges facing IoT layers and its protective measures. International Journal of Computer Applications, 975, 8887.

[13] Sha, Kewei, Wei Wei, T. Andrew Yang, Zhiwei Wang, and Weisong Shi. "On security challenges and open issues in Internet of Things." Future Generation Computer Systems 83 (2018): 326-337

[14] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.

[15] Wei, W., Yang, A. T., Shi, W., & Sha, K. (2016, October). Security in internet of things: Opportunities and challenges. In 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) (pp. 512-518). IEEE.

[16] Juels, A. (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 24(2), 381- 394.

[17] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653-659.

[18] Săndescu, C., Grigorescu, O., Rughiniș, R., Deaconescu, R., & Calin, M. (2018, September). Why IoT security is failing. The Need of a Test Driven Security Approach. In 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet) (pp. 1-6). IEEE.

[19] Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012, April). RFID technology and its applications in Internet of Things (IoT). In 2012 2nd international conference on consumer electronics, communications and networks (CECNet) (pp. 1282-1285). IEEE.

[20] Gao, H., Guo, Y., Cui, J., Hao, H., & Shi, H. (2012). A communication protocol of RFID systems in internet of things. International Journal of Security and its Applications, 6(2), 91-102.

[21] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[22] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

[23] Ren, L. (2014). Proof of stake velocity: Building the social currency of the digital age. Self-published white paper.

[24] Benvenuto, C. J. (2012). Galois field in cryptography. University of Washington, 1(1), 1-11.

[25] Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications,National Institute of Standards and Technology, 19-22.

[26] Liu, J. J., Huang, Y. L., Leu, F. Y., Pan, X. Y., & Chen, L. R. (2017, October). Generating dynamic box by using an input string. In International Symposium on Mobile Internet Security (pp. 17-29). Springer, Singapore

[27] Bulens, P., Standaert, F. X., Quisquater, J. J., Pellegrin, P., & Rouvroy, G. (2008, June). Implementation of the AES-128 on Virtex-5 FPGAs. In International Conference on Cryptology in Africa (pp. 16-26). Springer, Berlin, Heidelberg.

[28] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.

[29] Pawar, A. B., & Ghumbre, S. (2016, December). A survey on IoT applications, security challenges and counter

[30] Kumar, P., Zaidi, N., & Choudhury, T. (2016, November). Fog computing: Common security issues and proposed countermeasures. In 2016 International Conference System Modeling & Advancement in Research Trends (SMART) (pp. 311-315). IEEE.

[31] Svantesson, D. And Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26, 391-397. doi:10.1016/j.clsr.2010.05.00

[32] Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack

detection in cloud computing. Future Generation Computer Systems, 28, 833–851. doi:10.1016/j.future.2012.01.006
[33] Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16, 102-107. doi:10.1016/j.istr.2011.08.005
[34] Joint, A., Baker, E. and Eccles, E. (2009). Hey, you, get off of that cloud? Computer Law & Security Review, 25, 270–274. doi:10.1016/j.clsr.2009.03.001
[35] Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, 513- 521. http://dx.doi.org/10.1016/j.clsr.2012.07.002
[36] Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.
[37] Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.
[38] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193
[39] Petcu, D., Macariu, G., Panica, S. and Crăciun, C. (2013). Portable Cloud applications—From theory to practice. Future Generation Computer Systems, 29, 1417–1430. doi:10.1016/j.future.2012.01.009
[40] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616
[41] Serrano, M., Quoc, H. N. M., Hauswirth, M., Wang, W., Barnaghi, P., & Cousin, P. (2013, June). Open services for IoT cloud applications in the future internet. In 2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 1-6). IEEE.
[42] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. Information Security Journal: A Global Perspective, 27(3), 162-182
[43] Miloslavskaya, N.G., & Tolstoy, A.I. (2018). Internet of Things: information security challenges and solutions. Cluster Computing, 22, 103-119.
[44] Kuo, Y. W., Li, C. L., Jhang, J. H., & Lin, S. (2018). Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications. IEEE Sensors Journal, 18(12), 5187-5197.
[45] S. Kraijak and P. Tuwanut, "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends," 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), Shanghai, 2015, pp. 1-6, doi: 10.1049/cp.2015.0714
[46] Feng, X., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. International Journal of Communication Systems, 25(9), 1101-1102.
[47] Wei, W., Yang, A. T., Shi, W., & Sha, K. (2016, October). Security in internet of things: Opportunities and challenges. In 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) (pp. 512-518). IEEE
[48] Karame, G., Androulaki, E., & Capkun, S. (2012). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. IACR Cryptol. ePrint Arch., 2012(248).
[49] Yun, J., Goh, Y., & Chung, J. M. (2019, January). Analysis of mining performance based on mathmatical approach of PoW. In 2019 International Conference on Electronics, Information, and Communication (ICEIC) (pp. 1-2). IEEE.
[50] Bentov, I., Gabizon, A., & Mizrahi, A. (2016, February). Cryptocurrencies without proof of work. In International conference on financial cryptography and data security (pp. 142-157). Springer, Berlin, Heidelberg.
[51] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 3-16).
[52] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653-659.
[53] Tsai, K. L., Huang, Y. L., Leu, F. Y., You, I., Huang, Y. L., & Tsai, C. H. (2018). AES-128 based secure low power communication for LoRaWAN IoT environments. IEEE Access, 6, 45325-45334
[54] Shanthi Rekha, S., & Saravanan, P. (2019). Low-Cost AES-128 Implementation for Edge Devices in IoT Applications. Journal of Circuits, Systems and Computers, 28(04), 1950062.
[55] Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16(3-4), 102-107.
[56] Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6), 833-851.
[57] Rai, R., Sahoo, G., & Mehfuz, S. (2013). Securing software as a service model of cloud computing: Issues and solutions. arXiv preprint arXiv:1309.2426.
[58] Casola, V., Cuomo, A., Rak, M., & Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29(1), 387-401.
[59] Yun, J., Goh, Y., & Chung, J. M. (2019, January). Analysis of mining performance based on mathmatical approach of PoW. In 2019 International Conference on Electronics, Information, and Communication (ICEIC) (pp. 1-2). IEEE.
[60] Rehana, J. (2009, April). Security of wireless sensor network. In Seminar on Internetworking.
[61] Hu, F., Ziobro, J., Tillett, J., & Sharma, N. K. (2004). Secure wireless sensor networks: Problems and solutions. Rochester Institute of Technology, Rochester, New York, USA.
[62] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE
[63] Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017, May). Security challenges in IoT development: a software engineering perspective. In Proceedings of the XP2017 Scientific Workshops (pp. 1-5).

Md Sajid Bin Faisal has got his Bachelor of Science (BSc) in Computer Science & Engineering (CSE) at American International University- Bangladesh (AIUB) from the year 2017 to 2020. Currently he is doing his Master of Science degree in Computer Science from American International University-Bangladesh. He is a current general member of AIUB Computer Club (ACC) & got selected twice in the Dean's List of Honor of Faculty of Science and Technology, AIUB. He has an enthusiasm over the research field of IoT, Network Security & Cryptography, Graph Theory, Algorithms & basic applications of Mathematics in modern world problems.

Ahsan Habib was born in Chandpur, Chittagong, Bangladesh in 1997. He received his BSc degrees in Software Engineering from the American International University-Bangladesh (AIUB) in 2020. He was selected two times in the Dean's List of Honor of Faculty of Science and Technology, AIUB in his BSc. He completed his internship entire title 'Network Security Aspect Internet' at National Credit and Commerce Bank Limited (Head Office) department of IT Hardware & Infrastructure Division in 2020.

He got President Scout Award in 2013. He was a general member of AIUB Computer Club (ACC). His current research interest in Internet of Things (IoT), Network Security & Cryptography, Graph Theory, Block Chain, Big Data and Software Engineering.

Md. Aolad Hossain Anna completed his B.Sc in Computer Science & Engineering from American International University-Bangladesh, Dhaka Bangladesh. Currently he is working as a Jr. Software Developer in Nexdecade Technology (Pvt) Ltd. He is a general member of AIUB Computer Club. His current research interest in Internet of Things (IoT), Block Chain, Network Security, Big Data, Human Computer Interaction, Encryption Algorithm and Software Engineering.

Cynthia Rashid Simin Has completed her Bachelor of Science (BSc) in Computer Science & Engineering (CSE) at American International University -Bangladesh (AIUB). Currently preparing for her Master's degree. She is highly interested in IoT as a research area, Network Security and cryptography, various Algorithms and Data Structures, Software Quality Assurance and Testing.

Dr. Dip Nandi Has completed his Master Degree on Information Systems from The University of Melbourne, Australia in 2009. Later he finished his Doctor of Philosophy (PhD) in Computer Science from RMIT University Melbourne, Victoria, Australia.

Dr. Dip Nandi is the current Associate Professor and Honorable Director of Faculty of Science & Technology (FST), at American International University- Bangladesh (AIUB). He is a former lecturer at RMIT University Melbourne, Australia from the year 2010 to 2012. Dr. Nandi has a vast range of research activities and contributions in various filed of Computer Science and Multidimensional researches. His profound knowledge over many leading domains and areas include the concept of Algorithmic Design, Software Engineering model & process, Machine learning, Data Warehousing, E Learning are mostly notable. Dr. Dip Nandi also has his Contributions in Alzheimer's disease and Dementia detection using Neural Networks. The education-based researches are also his area of expertise.