IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 3, 2018, accepted October 16, 2018, date of publication November 1, 2018, date of current version February 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2876939

Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms

TARIQ AHAMED AHANGER[1], (Fellow, IEEE) AND ABDULLAH ALJUMAH[2], (Fellow, IEEE)
[1]College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[2]Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

Corresponding author: Tariq Ahamed Ahanger (t.ahanger@psau.edu.sa)

This work was conducted at Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia, during 2017–2018.

ABSTRACT The Internet of Things (IoT) is an evolving global trend in Web-based information architecture aiding in the exchange of services and goods over a network without necessitating human-to-human or human-to-computer interaction. It has the potential to revolutionize physical world interaction of individuals and the organizations. The application of IoT can be recognized significantly in many areas such as in healthcare, resource management, learning, knowledge processing, and many more. The practical realization of IoT is met with a plethora of security and privacy challenges that need to be tackled for IoT's successful deployment on a commercially viable large scale. This paper analyzes the security issues related to IoT networks through an analysis of the existing empirical researches to get an insight on the security requirements of the IoT networks. The findings of the study revealed that security threats are one of the biggest and ever-growing challenges for IoT, and it is essential to substantially mitigate them for the success of this platform.

INDEX TERMS Internet of Things (IoT), security, cyber-attacks, privacy, threats, cyber security.

I. RESEARCH CONTEXT

IoT is defined as an active global network architecture having self-configuring abilities based on standard and interconnected communication protocols, where both virtual and physical objects/things have identities, physical characteristics and virtual representation'(IERC, 2016 pp-3). This term 'Internet of Things' (IoT) was coined by Kevin Ashton, in the year 1999 and later was formally introduced in 2005 by the International Telecommunication Union (ITU).

It is a fast-growing network that will potentially transform the human lives and is the next big development in the internet technology. The fundamental concept of IoT is to attach embedded sensors or miniature devices to day to day objects/things to transform them into smart objects/things. Some of the key features of IoT includes mobility, wireless connectivity, embedded sensors, wide ranging of technological use and support for diverse devices [6]. IoT represents the parent class for virtual and physical things in the environment and enables intelligent communication integrated with information network. The four main features of IoT are sensing; information accessing; heterogeneous access, applications and services; and security privacy and trust [7].

IoT has become a buzzword in the business environment within little time and has gained tremendous popularity due to certain features like its ability to ease the operational process of businesses and instant communication. Subsequently its applications in different walks of life is seen to be rising significantly [2]. In past few years, the concept of IoT has been applied in greenhouse monitoring, smart electric meter reading, telemedicine monitoring as well as intelligent transportation [3]. IoT's potential of offering interconnection of ''things'' across the world through miniature systems and sensor networks offers global communication. To this, there arises concerns related to security, privacy and trust issues in trans-reception of the information [4].

II. NEED FOR THE STUDY

With changing technology and arrival of 5G network, IOT is the future of technology which will be powerful enough to move the mankind entirely into online world. This advancement in technology has already started to change face of technology like never before. It brings with it all positives like increased efficiency and effectiveness. But with all the positives, the biggest threat to IOT is the security threat in terms of invasion of privacy, unauthenticated access, denial of service and much more. Thus, it is important to understand as to what are the associated security threats of IoT as well as their potential solutions.

III. AIM OF THE STUDY AND METHODOLOGY

The main aim of this study is to analyze the security challenges and defense mechanisms against those challenges related to Internet of Things (IoT). The other objective of this study is to provide a brief overview of IoT applications in present times and to analyze the type of security threats and common cyber-attacks on the IoT applications.

The methodology of the study is based on empirical review of the available literature studies in relation to security challenges and potential solutions to the security threats of IOT. The researcher has chosen empirical review method to gain insight on the practical implication of security in the IoT applications instead of deriving knowledge from theories and beliefs.

IV. DISCUSSION

A. APPLICATIONS OF IoT

In present times, IoT is being applied in a wide range of applications including domestic monitoring, healthcare, environment sensing, agriculture and more. The application of IoT in configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others are discussed here briefly. IoT has also become a fundamental building block for smart objects/items, it aids in creating smart persistent cyber-physical systems [5]. IoT's application in smart living has the potential to improve the quality of life substantially [6].

Smart Homes based on IoT technology are aimed at providing additional personalized comfort, ecological sustainability and security. It uses a wide range of domestic sensors and large amount of data in making intelligent operational decisions for increasing comfort level and energy conservation [7]. IoT based smart and aware architecture for tracking patient records and automatic monitoring of the personnel is the basis of Smart Healthcare applications. In these applications, biomedical devices are used by hospitals as well as the nursing institutes to monitor the patients' vitals. Smart Healthcare Systems uses diverse yet harmonizing technologies, such as RFID, Wireless Sensor Networks, and smart mobiles [2].

Smart cities are one of the significant applications of IoT, in which a city functions in an intelligent and sustainable manner. In this application the entire infrastructure, heterogeneous technologies and services are integrated cohesively. The intelligent devices and wireless sensor networks are efficiently used here for monitoring and control through IoT network [8]. In addition to this IoT is applied in a wide variety of application domains such as smart grids [9], smart sensors in industrial environment [10], smart rehabilitation system [11], smart agriculture [12] to name a few, some applications of IoT are briefly discussed in Table 1.

B. SECURITY THREATS OF IoT

Some of the main security threats in IoT section is presented in this section and table 2 provides a brief empirical review on the same.

- ***Confidentiality:*** Confidentiality in digital environment is related to protecting user's identity and freedom from external intrusion. Confidentiality threats are generally invasion of user's privacy by getting an unauthorized access to confidential user data using various mechanisms [14]. Furthermore, unwanted disclosure of sensitive data is also a breach of confidentiality [3]. For the devices based on IoT the confidentiality threat is transmitting confidential data to neighboring noses or transmitting data to unauthorized user [15]. For every device and sensor in the IoT network has potential confidentiality breach risk associated with them. As any poor encryption scheme or backdoor access loopholes are potential threats for data confidentiality of several user on any network having potentially severe consequences [16].
- ***Integrity:*** Integrity of data refers to protection of the meaningful information (from cybercriminals) as well as errors occurring during transmission and reception in order to ensure credibility and accuracy of the data. While information is in the communication medium, it could be altered by the malignant users [16]. Significant errors due to channel imperfection, electromagnetic disturbances and instrumental limitations can also alter the information transmitted. In IoT devices, the integrity of data can only be maintained when its access
- by the permitted user is done on secure interface through a secure medium [7].
- ***Availability***: Availability of data is ensuring immediate access to information resources to authorized users. One of the main goal of IoT services is to provide data whenever required in both normal and crisis situations [17]. As IoT services are often used by large organization to get access to large amount of data, ensuring immediate data availability is one of the primary goal of IoT service providers. Denial of service attack and bottleneck situations are the primary availability threat for IoT service that can block the information flow and deny data to the end users [18].
- ***Authenticity:*** Authenticity is related to providing network access to only legit users. Authentication threats are related to tampering of control and sensing information used for gaining unauthorized access to confidential data. The unauthentic user can not only read the data but also can modify or erase it, destroying the integrity of data [14]. With IoT, authentication threats arise mainly due to lack of proper mechanism for authentication, tag cloning, spoofing and RFID eavesdropping. In addition to this authentication breach at the administrative level can compromise the entire network by denying legitimate users access, stealing of sensitive data, flooding of network and more [16].
- ***Non-Repudiation:*** Non repudiation is related to authentication of a legit party in getting access to the promised service. This threat is related to certain characteristics of IoT namely: autonomy, pervasiveness and ubiquity.

TABLE 1. Application of IoT.

Application	Features	Advantages	Challenges
Smart Homes	• Remote controlling of appliances • Customization of home environment • Centralization of control	• Save time • Energy conservation • Makes life convenient and simpler	• High costs • Handling of volumes of data generated • Data interpretation • Semantic Interpretation • Software complexity
Smart Cities	• Efficient traffic management • Efficient water distribution system • Better waste management • Improved urban security • Effective environmental monitoring	• Effective solution for traffic congestion challenges • Reduction in noise and pollution • Safer cities	• Self-organization in sporadic environment • Handling of volumes of data generated • Data interpretation • Interoperability • Security and privacy • Software complexity
Smart grid	• Analyzing capacity of electricity suppliers • Analysis usage pattern of consumers • Automation	• Improved efficiency • Cost-effectiveness • More reliable • Reduction in cost of electricity	• Interoperability • Fault tolerance
Smart healthcare	• Better connected health care system • Use of smart biomedical devices • Personalized remedies	• Access to quick healthcare • Better patient monitoring • Early detection and prevention of diseases.	• Handling of volumes of data generated • Data interpretation • Scalability • Software complexity • Security and privacy
1) Smart *2) supply chain* *3) and retail*	• Proximity-based advertising • Solutions for goods tracking • Better exchange of inventory information	• Saving search time • Lowering labor costs • Reduced inventory costs • Tracking customer behaviour	• Limited popularity • Scalability • Distributed computation
Smart sensors in industrial environment	• Use of RFID and NFC in large warehouse management • Energy efficiency • Predictive maintenance	• Streamlining infrastructure • Improved resource management. • Cost efficiency	• Lack of popularity amongst masses • Distributed computation • Fault tolerance
Smart agriculture	• Remote livestock monitoring • Sensing soil moisture • More accurate weather analysis • Reformed irrigation system	• Revolutionizing remote farming operations • Better handling of micro-climatic conditions for increased production • Improved water utilization	• Remoteness of the farm location • Lack of attention • Semantic Interpretation

TABLE 2. Review of literature for security threats in IoT.

Author name and year	Aim of paper	Findings
Babar et. al., (2010)[18]	This study had explored various security challenges for IoT	This study had discussed privacy, security and trust issues for both devices and information in IoT environment.
Suoa, Wana, Zoua, and Liua (2012)[17]	The main aim of this study is to analyze security issues for IoT applications	This study had concisely reviewed security issues in the IoT, by analyzing security properties and requirements for four architectural layers namely perceptual layer, network layer, support layer and application layer.
Jing et. al., (2014)[20]	This paper had analyzed the cross-layer heterogeneous security issues and respective solutions for IoT.	Security issues for three layers in IoT architecture namely, perception layer, transportation layer and application layer, was discussed here. This study had analyzed authenticity, confidentiality related challenges in IoT.
Cooper (2015)[19]	This study had analysed security issues in IoT	This study had discussed key challenges such as, Authentication, Authorization, Confidentiality and Integrity for IoT environment.
Oriwoh, Al-Khateeb, and Conrad (2015)[4]	This study had analyzed non-repudiation and responsibility in the resource-constrained IoT.	This study had concluded that responsibility and non-repudiation are feasible for IoT's cyber-physical eco-system in applications like digital forensics, cyber-crime investigations and such. This study pointed out that there is antrade off between basic security principles and resource constraints for authentication in IoT.
Farooq, Waseem, and Khairi (2015)[15]	The main aim of this study is to review the security and privacy challenges in a well-defined architecture of IoT.	This study had presented some challenges for the ubiquity of IoT. The security threats were analyzed for each architectural layer and special focus was on the requirement for confidentiality, integrity and availability of data.

The relationship between authentication and non-repudiation is essential feature for IoT that promises trustworthy communication. Attack on this feature of IoT environment includes loss of connection, resource constraints, waste of energy and resources. Under this attack, the protection against false receipt of message acknowledgement is compromised [4], [19].

Table 2 presents some of the important researches conducted on identifying security threats related to IoT empirically.

C. CYBER-ATTACKS ON IoT APPLICATIONS

Some of the most common cyber-attacks on the IoT applications are discussed here and table 3 provides a brief empirical review for the same:

- ***Sinkhole Attack:*** Sinkhole Attack is a kind of attack of network layer that occurs when data is routed during the transmission. Under this attack, all the data flowing through the network is diverted to one compromised node in the network [21]. This attack reduces the traffic flow, fooling the senders and network that the packet had been received at its intended destination. This attack is an active attack that can further lead up to Denial of Service (DoS) attack by creation of traffic and disruption of routing path [22].
- ***Wormhole Attack:*** Wormhole attacks are severe form of attacks that can be used against any protocol as it has ability to affect the encrypted traffic. This attack can cause failure in location detection, disrupt topology of

TABLE 3. Review of literature for cyber-attack on IoT applications.

Author name	Aim of paper	Findings
Pongle and Chavan (2015)[24]	The main of this study is to analyze real time intrusion and wormhole attack detection in IoT	This study had proposed a novel method for detecting wormhole attack and attacker. This method uses the node location information and neighbor information for securing against such attacks.
Mathur, Newe, and Rao (2016)[25]	The main aim of this paper was to analyze defense against black hole and selective forwarding attacks in Medical application of IoT	This study had proposed the use of cryptographic hashes method for neighbourhood watch as well as threshold analysis for detecting and correcting such attacks
Pawar and Vanwari (2016)[26]	This study had analyzed Sybil attack in IoT environment	This study had recognized sybil attack as a fundamental problem in IoT that has no universal solution. A defense scheme was presented in this scheme which included social graph-based sybil detection, behaviour classification-based sybil detection and mobile sybil detection.
Kaur and Singh (2016)[27]	The main aim of this study was the detection and prevention of HELLO FLOOD attack.	This study had presented use of centralized techniques for wireless sensor network in order to detect and prevent hello flood attacks.
Stephen and Arockiam (2017)[22]	The main of this study is to present an intrusion detection system for detect Sinkhole Attack in IoT environment.	This study revealed that connection with the wireless sensor network is prone to sinkhole attacks. An intrusion detection system used RPL protocol and alerts the leaf to reduce packet loss.

the network and cause routing failures. Under this attack attackers forms a tunnel between two attackers and all the traffic is transmitted through it. Packet encapsulation and packet relay are used by the attacker in this form of attacks [23], [24].

- ***Selective Forwarding Attack:*** The selective forwarding attack is a version of black hole attack. Under this attack one or multiple nodes of the network are captured by the attackers. When any one of the node drops malicious packet as a selective forwarding attack, others help in covering the attack. It causes packet losses due to resultant interferences and is difficult to detect. This attack can cause transfer of incomplete information risking its integrity. Also in some applications incomplete information can be more dangerous than the no information of the same [25].
- ***Sybil Attack:*** Sybil attack is another of the network layer attack, in this attack the nodes are manipulated by the attackers and multiple identities for a single node. This kind of attack compromises the entire system that can result into redundancy and false information [16]. In IoT network, sensors are embedded on the objects, which integrates sensing with communication and under this attack fake identities are generated. These fake identities can produce wrong reports, increase traffic load with spam and loss of privacy can also occur due to malware and fishing under this attack [26].
- ***Hello Flood Attack:*** A most common assumption made by multiple protocols when receiving a HELLO packets is that the receiver is within the radio range of the receiving device and is considered as neighbor. An attacker with the use of high-powered transmitter can trick the nodes of network in believing it is a neighbor and falsely broadcast to all nodes of the network. Under this attack, attacker can cause every node to mark malicious node as the parent node, which can cause a huge loss of data traffic, spoof routing routes and increase traffic in the network [27], [28].
- ***Denial of Service (DoS) Attack:*** DoS attack can occur both at network and application layer of the network. Under this attack the network is flooded by the attacker with useless data traffic intended for exhausting network resources. This attack causes network to be unavailable to the authentic users [29]. At the application level this attack has become more refined, where the defense mechanisms of the networked are breached and the sensitive information stolen in under control of the attacker. This attack can also lead up to

shutting down of the entire network making it completely unavailable [16].

Table 3 presents some of the important researches conducted on such attacks related to IoT empirically.

D. SET OF SECURITY REQUIREMENTS REQUIRED TO MAKE IoT SECURE- EMPIRICAL ANALYSIS

This section presents the empirical analysis of the existing studies related to security and privacy concerns in IoT environment.

Babar *et al.*[18] presented a security model for IOT in a study titled ''Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)''. A taxonomical overview of security and privacy concerns in IoT is presented here. The authors have proposed a cube structured model for converging security, privacy and trust in IoT environment. This model considers the composite and complex nature of IoT environment in mitigating all the concerns of authorization, response and reputation related to IoT. This proposed integrated method was for tackling key challenges of authentication, identity management and embedded security. This study recognized security requirements for IoT namely, resilience to attacks, data authentication, access control, client privacy, user identification, identity management, secure data communication, availability, secure network access, secure content, secure execution environment and tamper resistance.

A study was presented by Weber [14] titled ''Internet of Things – New security and privacy challenges'', which considered legal security requirements of IoT. This study elaborated on the need for measures adaptation for data authentication, access control, preserving privacy and resilience towards attack. This study also emphasized on the requirement for a legal framework as per the international standards for the underlying technology used in the network.

Zhuo and Chao [30] had presented a security architecture in a paper titled ''Multimedia Traffic Security Architecture for the Internet of Things''. This paper had presented a novel security architecture capable of handling heterogenous application using a Media-aware traffic security architecture (MTSA) model. The model proposed also provided a favorable trade-off between network efficiency and trade-off. In addition, security measures such as Batch Rekeying, Watermarking and Authentication control were also discussed here.

Suoa *et al.* [17] presented a review study titled ''Security in the Internet of Things: A Review''. This study had reviewed the progress of IoT with the focus on the security of this ecosystem. A deep analysis of security features and architecture was presented in this study. The paper had discussed key security technologies such as encryption methods, communication medium security, use of cryptography and protection of sensor/control data for tackling the major security and privacy threats.

A similar study was presented by Kozlov *et al.* [16] titled ''Security and Privacy Threats in IoT Architectures''. The authors had termed IoT as the upcoming ubiquitous technology. This study had analyzed the security and privacy threats at different level of IoT system architecture, including both attack centric and system failure centric threats. This study had also analyzed security, privacy and trust issues in both the top-bottom and bottom-top IoT infrastructure construction. It also analyzed energy consumption of IoT network and its link with various security, privacy and trust issues in the architecture. The authors had referenced to EU directive 95/46/EC and emphasized on data protection laws within the IoT networks. It had promoted prohibition of individual profiling, supporting provisions for erasing personal and accepting anonymity and pseudo-anonymity of data.

Keoh *et al.* [31] presented a paper titled ''Securing the Internet of Things: A Standardization Perspective''. This paper discussed the security aspects of the IoT deployment and emphasized that proprietary solutions of security are not coherent for providing standardize security in IoT environment. This paper had provided a detailed review on the communication security for IoT and the standard protocol proposed is based on Constrained Application Protocol (CoAP), which is an application protocol catering to the limitations and requirement of IoT devices. The proposed model had used Datagram Transport Layer Security (DTLS) for security under proposed model. This paper had presented detailed application of DTLS in public key, protecting group communication and complexities in implementation. Additionally, packet fragmentation challenges in DTLS are also discussed here.

Abomhara and Koien [32] had presented a study titled ''Security and privacy in the Internet of Things: Current status and open issues''. This paper had discussed open challenges and security concerns in IoT domain. An author has shed light on present state of security in IoT environment as well as discusses the futuristic directions for tackling security and privacy concerns. The authors had presented set of characteristics for security and privacy measures such as cost-effectiveness, credibility and efficiency for protecting integrity, ensuring confidentiality and integrity of information.

Alqassem [29] presented an article titles'' Privacy and security requirements framework for the internet of things (IoT)''. This study discusses the early stage security and privacy requirements of IoT. The framework proposed in this study was aimed at building effective model that can handle the heterogeneity of IoT network by tackling the privacy and security concern at earliest stage possible.

Security design challenges were discussed by Xu *et al.* [21] in a paper titled ''Security of IoT Systems: Design Challenges and Opportunities''. This paper had analyzed application of Computer-aided design (CAD), for secure Internet of Things (IoT) environment. This paper had discussed rarely addressed security issues such as reliable sensing, secure computation, communication links, privacy as well as digital forgetting. Additionally, security risks posed by sensors, actuators and other common components of IoT on accuracy and integrity

TABLE 4. Empirical review for set of security requirements required to make IOT secure.

Author name and year	Aim of paper	Findings
Babar et. al., (2010)[18]	This paper aims to provide an overview, investigation and classification of various security and privacy issues associated with IoT.	This study proposed a cube structured model for converging security, privacy and trust in IoT environment
Weber (2010)[14]	The main aim of this study is to assess IT-security-legislation and provisions for the use of IoT	This study had discussed new regulatory approaches for IoT, ensuring privacy and security. This study emphasizes that data authenticated, interception of attacks have to be intercepted, access controlled, and privacy protection of user are essential for IoT.
Zhuo& Chao (2011)[30]	The main aim of this study is to address the vital challenge of supporting multimedia applications in IoT in a secure manner.	A multimedia traffic analysis and method was proposed to securely handle heterogeneity in diverse applications. The proposed model had good trade-off between system efficiency and flexibility.
Suoa et. al., (2012)[17]	The aim of this study was to deeply analyze security characteristics and architecture of IoT.	This study had outlined key security challenges and had discussed the status of main security technologies such as encryption, safe communication, protection of sensor data and cryptographic.
Kozlov, Veijalainen& Ali (2012)[16]	This study had analyzed the Security, privacy and trust infrastructure in both bottom-up and top-down construction approaches.	This paper had presented a layered view on the threats related to security, privacy and trust architecture. It had also reviewed EU legislation in privacy and security area and its importance for IoT domain.
Keoh, Kumar & Hannes (2014)[31]	This paper aims to provide an on standardization of the security solutions for IoT ecosystem.	This study had a detailed review on various communication security solutions in IoT and had proposed the use of Constrained Application Protocol (CoAP) with standard security protocols.
Abomhara&Koien (2014)[32]	This study had analysed the current issues related to security and privacy in IoT	This study had revealed that accuracy, confidentiality, integrity, authentication, and access control are the vital for enabling credibility, security, and privacy economically and effectively in IoT environment.
Alqassem(2014)[29]	This study had analyzed privacy and security requirements in IoT	This study had presented a methodological framework to meet the the privacy and security requirements in IoT and this model had proposed to tackle such threats at the earliest stages.
Xu, Wendt &Potkonjak (2014)[21]	The main aim was to conduct a survey study for analyzing security challenges and opportunities with IoT.	This study had analyzed various IoT security protocols and proposed a hardware-based approach. This study had provided a starting-points in developing CAD based security solutions.
Lin & Bergmann (2016)[7]	This study had analyzed privacy and security concerns related to IoT in smart home environment	This paper had recognized two main auto-management technologies for enhancing system security namely auto-configuration and automatic updating of software and firmware for secure operations. This study also highlighted need for efficient security policies and methods for maintaining automation.
Zhou et. al., (2017)[3]	This study presented challenges related to security and privacy in cloud-based IoT	This study had analyzed both practical and academic requirements in cloud-based IoT and had proposed a novel effective privacy-preserving method for achieving secure data collection from multiple heterogeneous users.

of physical signals were also discusses here. This paper elaborates upon CAD based security techniques and other hard-ware based security strategies for secure IoT networks.

Lin & Bergmann (2016) had presented an article discussing security issues related to IoT's application in Smart Homes, titled ''IoT Privacy and Security Challenges for Smart Home Environments''. This study had differentiated the security and privacy requirements of a commercial infrastructure to the domestic requirements of Smart Home. In addition, financial resources and human resources required to employ security and privacy protection solutions in Smart homes were also discussed here. A survey was conducted by the authors for analyzing existing IoT security solutions and their appropriability for Smart Home environment were discussed here. The authors have presented a gateway architecture for resource-limiting devices and high availability of system. Two main aspects of auto-management were first the auto-configuration for enhancing system security and second, the automatic updating of firmware and system software and firmware for ensuring safe operations.

More recently Zhou *et al.* [3] presented a article titled ''Security and Privacy for Cloud-Based IoT: Challenges''. This article shed light on the security concerns arising due to unique characteristics of IoT of resource such as, resource limitations, self-organization, and short-distance communication. This leads to IoT reliance on cloud for storage and computation increasing the threats to privacy and security. In addition to this, this study had discussed the limitation of existing security measures and has elaborated on the security requirements of next-gen IoT services. The focus was on the challenging issue of privacy preservation, authentication and secure packet forwarding.

Table 4 reviews these studies systematically.

V. CONCLUSION OF THE STUDY

The Internet of Things (IoT) has the potential to connect billions of devices, irrespective of time and place to the World Wide Web. It also has potential to redefine physical world communication conducted by individuals, public and private organizations. Potentially, IoT devices will surpass the number of mobile phones and personal computers by a huge margin. As IoT environment will potentially cater billions of devices and will have access to enormous information which attracts data-hungry adversaries. This has necessitated the requirement for proper privacy and security measures in IoT networks.

Loopholes in security can be leveraged by hackers or attackers to carry numerous malicious or nefarious activities such as, leaking of confidential and sensitive data, denying access to the legitimate users, locking the system for administrators, circulation of wrong or malicious data, financial frauds, loss of control over entire IoT ecosystem and several more. As IoT has gained popularity with several industries and products are being developed to meet the market requirements for gaining more benefits.Thus, lack of security measures can impact the usability of this technology on a large scale. Additionally, data is a vital asset of present times, lack of security can result into violation of integrity of data that can led economical loses to organization utilizing such data.

This study presented an analysis of various security threats on IoT networks and discussed possible solution to tackle the same. In sync with the existing literature studies, this study also recognized security, privacy and trust issues primary amongst the paramount constraints in IoT services and networks. One of the main features of IoT recognized in this study is that it is not a single application platform but supports multiple technologies and services. The various application of IoTas seen in smart city, smart home, smart health care indicates its growing importance.

Many research studies have been conducting on analyzing security and privacy threats in IoT environment. Thus, through the review of existing literature studies, the researcher yielded quite crucial findings that aided in gaining insight on the concept of IOT, its applications and the security and privacy concerns related to it. Some of the existing literature studies had particularly discussed and categorized the privacy and security threats at different layers/levels of the IoT architecture. Thus, it was also noted by the researcher that security and privacy threats at all the architectural levels are expository for IoT functioning.

Some of the common security breaches recognized by this study were related to confidentiality of data, integrity of data, secure user authentication, and secure access control and such. This finding had been supported by majority of the existing research study after concisely reviewing security mechanisms in the IoT as well as analyzing security, privacy and trust characteristics and futuristic requirements of the network. Few of existing research studies presented security architecture for IoT that proposes security mechanism for each logical level to tackle threats. This approach is regarded as stable-persisting solution that can strengthen in-depth defense mechanism of the system. In some of the existing literature studies, recognition to various form of privacy breaks in the form of breach of user's query privacy, identification of user's location, node capturing and many more reflects the severity of the security challenges underlying IoT. Also it was noted by the researcher that privacy and trust breaches along with the security breaches are also critical aspect for IoT ecosystem.

A few of existing studies had also elaborated on a need for global standardization of security protocol for the success of IoT ecosystem. There has been many achievements in implementation of effective security infrastructure in IoT environment in recent times. Some of the research studies have emphasized on the requirement for attacks to be intercepted, data to be authenticated, controlling access to network and preserving privacy of customers. Nevertheless, many researchers emphasized that these advancements are required to be expanded further to seek new and more efficient potential security solutions. This in turn has the capability of thwarting ever-evolving data-hungry and malicious attackers.

As IoT applications can be accessed by multiple domains and has multiple user regimes, it requires security framework that enables users to have confidence in the data and services exchanged over the platform. Additionally, it is essential for security framework to distinguish between human and machine users without denying access to legitimate users. Most of companies employing IoT, requires security mechanisms for advances in the areas of lightweight public key management, encryption algorithms, resource constraints, trust control, access control and associated authorization schemes. In addition to this, new approaches use of machine learning/artificial intelligence in management of IoT, homomorphic encryption, searchable encryption and more are also promising security methods for this platform.

Overall, this study provided significant insight on the various current issues related to security threats on the IoT environment and presented existing solutions exist for tackling these security issues. However, in the opinion of the researcher, these solutions are marginally justifiable for high-level security requirements. Even though some of the measure can mitigate few security risks significantly but elimination of those concerns is yet to be achieved. In the opinion of the researcher, the existing security solutions are required to be improved upon, owing to the growing potential of attackers and increasing risks with the popularity of IoT

REFERENCES

[1] *Towards a Definition of the Internet of Things (IoT)*, IEEE, Piscataway, NJ, USA, 2015.

[2] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015.

[3] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[4] E. Oriwoh, H. M. Al-Khateeb, and M. Conrad, "Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios," in *Proc. Int. Conf. Comput. Technol. Innov. (CTI)*. Luton, U.K.: Univ. of Bedfordshire, May 2015, doi: 10.13140/RG.2.1.4030.3124.

[5] G. Fortino *et al.*, "Integration of agent-based and Cloud Computing for the smart objects-oriented IoT," in *Proc. IEEE 18th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, 2014, pp. 493–498.

[6] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016.

[7] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[8] R. Petrolo, V. Loscrí, and N. Mitton, "Towards a smart city based on cloud of things," in *Proc. ACM Int. Workshop Wireless Mobile Technol. Smart Cities*, 2014, pp. 61–66.

[9] F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for IoT application on smart grids: Survey and research challenges," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2016, pp. 63–68.

[10] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. D. Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1417–1425, May 2014.

[11] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1568–1577, May 2014.

[12] F. Tongke, "Smart agriculture based on cloud computing and IOT," *J. Converg. Inf. Technol.*, vol. 8, no. 2, pp. 1–7, 2013.

[13] K. A. M. Zeinab and S. A. A. Elmustafa, "Internet of things applications, challenges and related future technologies," *World Sci. News*, vol. 67, no. 2, pp. 126–148, 2017.

[14] R. H. Weber, *Internet of Things—New Security and Privacy Challenges*. Amsterdam, The Netherlands: Elsevier, 2010.

[15] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015.

[16] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in IoT architectures," in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 256–262.

[17] H. Suoa, J. Wana, C. Zoua, and J. Liua, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, 2012, pp. 648–651.

[18] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," in *Recent Trends in Network Security and Applications*. Berlin, Germany: Springer-Verlag, 2010.

[19] A. Cooper, "Security for the Internet of Things," School Comput. Sci. Commun., KTH Royal Inst. Technol., Stockholm, Sweden, Tech. Rep. 848663, 2015.

[20] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.

[21] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, 2014, pp. 417–423.

[22] R. Stephen and L. Arockiam, "Intrusion detection system to detect sinkhole attack on RPL protocol in Internet of Things," *Int. J. Elect. Electron. Comput. Sci. Eng.*, vol. 4, no. 4, pp. 16–20, 2017.

[23] S. D. Bhosale and S. S. Sonavane, "Wormhole attack detection in Internet of Things," *Int. J. Eng. Technol.*, vol. 7, no. 2, pp. 749–751, Jun. 2018.

[24] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in Internet of Things," *Int. J. Comput. Appl.*, vol. 121, no. 9, pp. 1–9, 2015.

[25] A. Mathur, T. Newe, and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT," *Sensors*, vol. 16, no. 1, p. E118, Jan. 2016.

[26] S. Pawar and P. Vanwari, "Sybil attack in Internet of Things," *Int. J. Eng. Sci. Innov. Technol.*, vol. 5, no. 4, pp. 96–105, 2016.

[27] P. Kaur and E. J. Singh, "Detect and prevent HELLO FLOOD attack using centralized technique in WSN," *Int. J. Comput. Sci. Eng. Technol.*, vol. 7, no. 8, pp. 379–381, 2016.

[28] S. Millar, "Network security issues in the Internet of Things (IoT)," Queen's Univ. Belfast, Belfast, U.K., Tech. Rep. 13616005, 2016.

[29] I. Alqassem, "Privacy and security requirements framework for the Internet of Things (IoT)," in *Proc. 36th Int. Conf. Softw. Eng. (ICSE Companion)*, 2014, pp. 739–741.

[30] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the Internet of Things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, May/Jun. 2011.

[31] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014.

[32] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *Proc. Int. Conf. Privacy Secur. Mobile Syst. (PRISMS)*, 2014, pp. 1–8.

TARIQ AHAMED AHANGER is currently an Assistant Professor with the Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University. He has authored over 40 referred papers. His interests include Internet of Things, cyber security, and artificial intelligence.

ABDULLAH ALJUMAH is currently a Professor with the Department of Computer Engineering, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University. He has authored over 40 referred papers.