A Security Model for IoT based Systems

Z. Safdar[1], S. Farid[2], M. Pasha[3], K. Safdar[4]

[1,3]*Information Technology Department, Bahauddin Zakariya University, Multan, Pakistan*
[2]*Computer Science Department, Bahauddin Zakariya University, Multan, Pakistan*
[4]*Computer Science Department, Air University, Multan Campus, Pakistan*
[2]shahidfarid@bzu.edu.pk

Abstract-Internet of things is novelemerging Internet based system for the exchange of information to provide efficient services regardless of time and place. IoT technology is playing a vital role in the current environment due to its wide spread applications in every domain of life like industrial, social, health care and domestic applications. IoT directly affects the security and privacy of all its involved entities as reported in the literature. Therefore, this study aims to propose a Security Enabled Model to provide secure end to end communication in IoT environment. Intensive literature review has been conducted to identify and investigate various security and privacy challenges encountered by the IoT environment. Proposed model ensures security at each layer of IoT. These layers includes I) perception layer which provides authentication process for the identification of fake objects ii) network layer that emphasis on data security process through cloud platform and iii) application layer which provides authentication for the end users. Results show that small sensing devices need to be highly focused in order to make them more secure and lightweight encryption techniques need to be developed. Furthermore, sensing devices are required to be more secure and protected from unauthorized access.

***Keywords-*:** IoT, Object Identification, Authentication, Security Enabled Model

I. Introduction

Internet of Things (IoT) include Smart devices, sensor networks and wearable devices with the purpose of exchanging information and services whereas sensor networks are the key for creating smart environments [i-v]. IoT systems are growing rapidly due to the rapid increment of wireless networks and enhanced range of sensing devices. IoT technology deals with millions and billions of sensing objects, machines and virtual entities that interact with each other. IoT technology is rapidly gaining attention by the practitioners and it is expected to have more than 100 billion interconnected IoT devices by 2020 [vi-ix]. In IoT data is collected from sensing objects that contain bulk data of structured or un-structured format that is managed through cloud platform services [x]. Collected data is transferred from objects to server for the storage and processing so that data would be available for visualization. IoT data resort towards cloud for the outsourced processing, storage that has brought a series of emerging challenging of security and privacy [ii, xi-xiii].

IoT is heterogeneous in nature (as shown in Figure 1) that increases complexity of security and privacy mechanisms so enhanced security protocols and crypto system are required [xiv] in order to ensure the secure interaction between the objects. Therefore, security is one of the key challenges that must be inhibited in order to drive IoT in real world. Moreover, security incidences that are resulted from bugs are software vulnerability that can cause huge damage to the whole networks. Vulnerability leads to a lot of more backdoor issues and let hackers attack on the network. Security challenges of IoT technology include object identification for fake objects, authentication, trust management, data confidentiality, network security and access control [i, ii, vi, xi, xv-xxxi]. The first malware issue in IoT was reported in 2013 [xxx] which highlighted the need to create a secure environment for small IoT objects to protect them from malicious attacks. Traditional symmetric and asymmetric encryption key distribution schemes cannot be applied to billions of IoT devices. Hence, a novel reliable and scalable key management scheme is required that leads to seamless interoperability between different networks and is vital for IoT system integration of big-data in cloud environment [xxiv, xxxii-xxxiv]. Therefore, this study focused on the identification and analysis of security challenges encountered by each layer of IoT architecture. Furthermore, this study contributes to fashion by proposing a novel model in order to cope with the end to end security challenges confronted by the IoT technologies through identification of each object.

This study is alienated as section 2 provides literature review of current security and privacy work in IoT, section 3 discusses identified challenges and Section 4 delineates the proposed model. Whereas Section 5 elaborates future work and Section 6 concludes the paper.

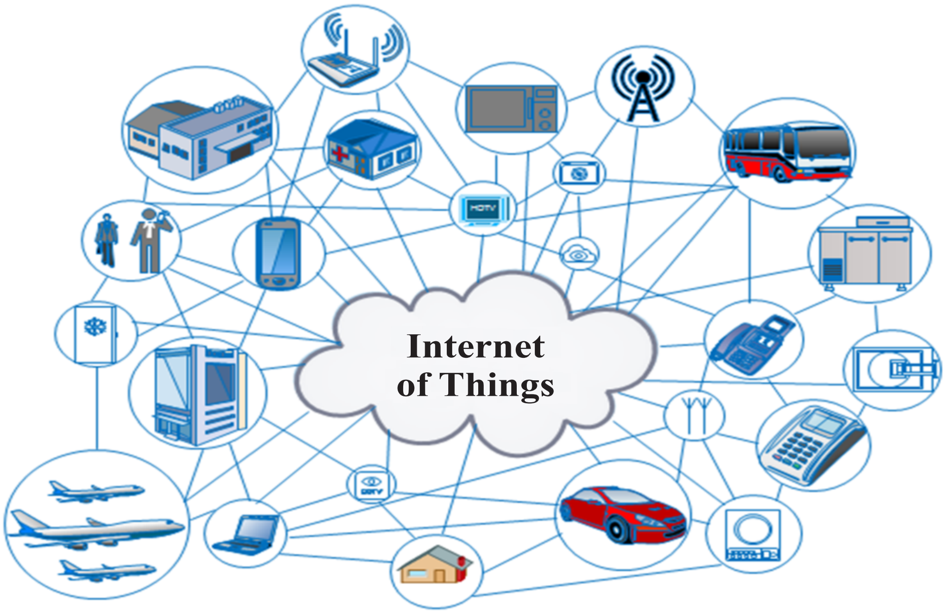

Fig. 1. Fundamental elements of IoT

II. Literature Review

The term IoT was coined by Kevin Ashton [ii, xii, xxxv-xxxvii] in late nineties. According to another definition [v] IoT is"A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query their state and any information associated with them, taking into account security and privacy issues". To Extend IoT include various technologies and sensors by which it facilitates exchange of things, such as goods, information and services between machines and human beings in more reliable and secure way. IoT sensor objects have simple structure, processors and high heterogeneity. IoT system collects real time data from Radio Frequency Identification Devices (RFID), public security, Laser Printer and Scanners, Global positioning Systems (GPS), logistics, intelligent building, healthcare including sensors such as body sensors, infrared sensors, Smart Meter, environmental monitoring and other embedded sensing devices etc. [ii, viii, xv, xvii, xxvii, xxxi, xxxviii-xl]. Then collected data is processed for identification, control of objects and management. IoT technology must have three characteristics that include reliable transmission of data over the network, intelligently processing the data before storing in data centers and comprehensive perception of store data from everywhere [xxxi].The cost of sensor objects effect all the working, if cost is too low it reduce the performance of overall network and make it less secure. High cost sensor objects improve the performance as well as increase cost of network maintenance. Fog computing is a new emerging trend which aims to reduce persuading service through moving the cloud services towards edge of the network. In recent years fog computing vision and key qualities have been outlined by many researchers. Fog computing is a stage to convey a rich portfolio of new applications and services at the edge of the system [xlii, xliii]. Generally, IoT structure is separated in three type of layers that include Application, Network or Transmission and Perception layer [xxxi]. Perception Layer intends to acquire, collect, process and store data from different wired or wireless objects [xli]. Data is collected from physical world that include different sensing devices, networks, RFID tags, wearable devices etc. Moreover, these devices monitor state of the physical environment and store it continuously [xii]. Perception layer is the initial source of IoT system that includes different technologies for the collection of data including short range radio technologies, device identity, signal detection, and connection with devices. The collected data is transferred through the network/transmission layer using Bluetooth, 2G, 3G and other technologies. Data is transferred from one place to another based on traditional communication networks for the integration of perception and communication networks [xli]. Network/transmission layer transfer data to the application layer that intends to process data and management of services [xli]. Application layer provide various services to all kinds of its users.

Requirement of privacy and security in IoT technology is most important concern for its stakeholders. IoT structure must support its characteristics for protecting data from unauthorized access. Each layer of IoT structure face challenges for providing security and privacy. These issues of IoT are directly related to its wide spread systems and applications. Fulfillment of these requirements is quite difficult and requires different technologies to meet security and privacy goals. The challenges that IoT structure is facing at each layer have been identified and depicted in Fig. 2. Identified issues/challenges must be resolved for providing a secure and protected IoT system.

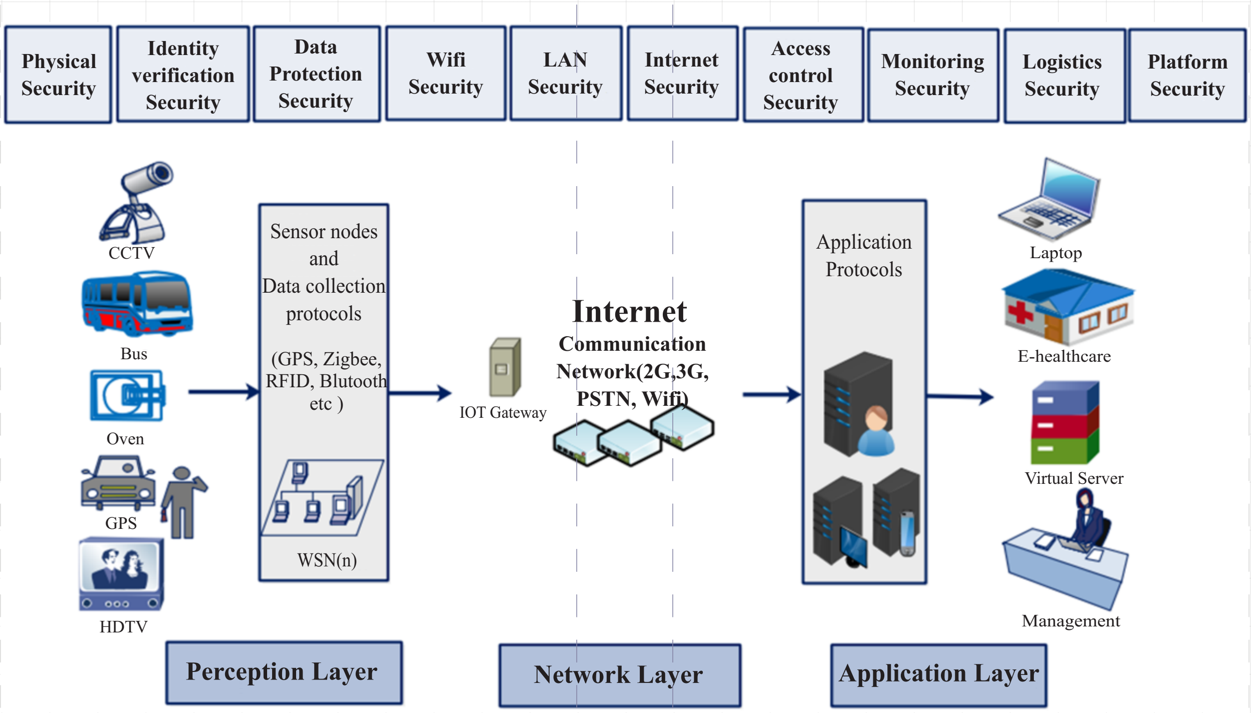

Fig. 2. IoT Architecture concerning Security and privacy

Many researches have proposed Architecture of this masive foundation of fog computing and storage and it also manage administration of the Fog objects. It is predicted that in coming years Internet of Everything (IoE) gadgets will be furnished. IoE will have wireless network interface cards for each heterogeneous device that include remote system interface cards through which energy efficient transport protocols will be designed[xliii].

TABLE I
COMPARISON OF IoT SECURITY ALGORITHMS

Algorithm	Function	Reference
AES	Confidentiality	[i, ii]
ECC	Digital signatures	[i]
RSA	Digital signatures	[i]
DH	Key agreement	[i]
SHA	Integrality	[i]

So far there is a notable and generally trusted suite of cryptographic algorithm connected to web security conventions as shown in Table I. Advance Encyption Standard (AES) has been used to maintain the confidentiality. Rivestshamiradelman (RSA) and Elliptic curve cryptography (ECC) algorithm has also been used to encrypt data by using digital signature and key transport in the network. Diffie Hellman (DH) and Secure Hash Algorithm (SHA-1/SHA-256) are used to maintain the integrity in the network. The importance of security and privacy related requirements have been addressed [xxix, xliv] for enterprises which have adopted IoT technologies. Furthermore, technologies for enhancing privacy, legal courses of action and state law scenarios have also been discussed. An other effort has been made[xxiii] in furnishing diverse levels of IoT security. Whereas a model for the perception layer have been placed forward for attacks. Later on [xxxi] a description was provided about IoT security architectures with their features and state problems related to diverse layers of IoT. Moreover, eachIoT layers' security measures have been discussed to provide better mechanism for security. Afterward each IoT layer security problems with solution have been outlined [xx]while security architecture was proposed and various security issues of IoT at various platforms were addressed [xxx]. A concise description of major challenges was proposed for full expansion of IoT devices and access control mechanisms for distributed devices werealso proposed for capable distributed devices [vi]. Subsequently, [xv] literature highlighted diverse aspects of IoT including existing security issues and open research challenges were included. Later on, [xiv] research provides an impetus for designing and developing security techniques for IoT Computer-Aided Design through highlighting different physical IoT devices challenges and opportunities. Additionally, privacy and trust relationship have been analyzed [xviii] while a formal model was proposed to link privacy with trust and it maps their relationship to maintain privacy relation in IoT systems. A confined solution to the security challenges of IoT had been proposed [xxvii] which focuses industries only. On the other hand, [xxvi] researchers proposed a trust management system considering the unsolved IoT security challenges. An efficient and scalable encryption protocol and protection techniques for heterogeneous devices was also proposed [xvi]. Whereas social aspect of implication of IoT in society was addressed including confidentiality and authentication etc. [xxii]. However, issues associated with secure packet forwarding includes privacy protection, authentication, cloud-based IoT cell phone technologies, their architectures and their requirement for security and privacy were also identified [xi]. Various challenges and solution of security, privacy, trust and robustness in location based devices have also been tackled [xvii] further it emphasized a wide range of policy regulations, privacy features in localization base devices for providing more secure and robust services.

Current literatures have only discussed the security and privacy challenges being faced by the diverse layers of IoT environment. Different security and privacy challenges of IoT system have only been discussed. Moreover, the existing models are confined to highlight the challenges without providing any mechanism to solve them. To the best of review and knowledge, there is no such security model that cover each layer's challenges [xxiii]. Therefore, the model proposed in this study ensures security at the diverse layers of IoT that has never been done before.

A. Security

Current research in IoT does not properly investigate security and privacy requirements for maintaining users trust. The main focus was to outline the challenges encountered by research community but no significant mechanism was devised to deal with problem [xx, xxvi, xlv, xlvi]. Existing IoT environment devices have no prior knowledge about one another so it is a big challenge to identify fake objects. Hackers and intruders have bad intensions for accessing devices data and changing information and software in IoT that can affect operational behavior of connected devices. Another challenge was to avoid user's privacy misuse [xxvi, xliv]. According to the review, Smart phones were sensor based devices that contain GPS, embedded sensors, proximity sensor, and gyroscope that are prone to security flaws. These devises lack data security and privacy in many cases [xvi, xli]. The critical areas of IoT include providing users personal data security, its availability, and query privacy, providing security at the vast collection of data and then protecting against legitimates is the critical challenge of IoT. Since IoT formed by the smart objects with autonomous facility in real time and spread the services all over the world, it required suitable solutions for ensuring the security goals of confidentiality, integrity and availability [xiv]. To ensure the availability to right people, strong access control and authentication systems with footprint supported by smart devices was highly required.

B. Privacy

Privacy includes personal information about identifiable participants. In IoT, increasing amount of participants, data, and communicating devices led to the need of privacy preservation mechanisms. Providing privacy of data were critical topics in sensing devices [x, xiv, xxvi, xlvii]. Technical approaches were required for the protection of participants' data. Next, in IoT main challenge was to provide application data protection, identity and access management, firewall, data encryption, privacy enhancing interaction, Radio Frequency Identifiers (RFIDs), Global Positioning System (GPS) and Near Field Communicators (NFC) which contain important characteristics associated with participants location[xxi, xxvi, xlviii-l]. Sometimes participants want to hide their personal information regarding location etc., but In IoT environment it becomes difficult to hide location on participants demand. So, as per the researcher, a trustable system was one that has analyzed all the risks and whose security and privacy issues had been settled [xxvi, li]. Trust look upon to the users 'faith', 'expectation', 'anticipation', 'confidence' and belief on the consistency and reliability of all the services provided by service providers. A trustable system must insure its users that their data would be with authorized service provider [xviii, lii].New Privacy Enhancing technologies (PET) had been developed for achieving these goals such as Virtual Private Networks (VPN) that is established by groups business partners, Transport Layer Security (TLS) TLS connection was required for providing confidentiality and integrity, DNS Security Extensions (DNSSEC) use shared public and private keys for providing integrity and authentication, onion routing encrypts data in multiple layers and wrapped it with covers of encrypted data and Private Information Retrieval (PIR).But providing security to all objects had become difficult in IoT environment[xxix, liii].

Hence, a novel reliable and scalable security model is required to authenticate each and every object that become a part of IoT environment that leads to seamless interoperability between different networks. Therefore, this study focused on the identification and analysis of security challenges encountered by each layer of IoT architecture. Furthermore, this study contributes in such a manner that proposes a Security Enabled Model in order to deal with the security challenges confronted by the IoT system through identification of each object. Proposed model includes security at each layer.

III. IDENTIFIED SECURITY AND PRIVACY CHALLENGES

Currently billions of people daily use internet but there are only few people who have knowledge of its working. Internet of things (IoT) connects various heterogeneous devices through internet that capacitate IoT devices with new capabilities. The amount of these heterogeneous devices is increasing every day that lead towards less reliability, adaptability, security and trust [xi, xxii, liii].Traditionally, the security mechanisms can't be devised to IoT technologies, because of its diverse communication standards and protocols. So these devices may not be protected under these mechanisms. These devices can be attacked and analyzed to reveal personal information. Security and privacy of users data needs to be ensured to stop access of illegitimate users along with access control, integrity, validation and verification mechanisms. Security challenges include object identification, authentication, authorization, privacy, security protocols, software vulnerability, privacy, malware in IoT etc. To provide most secure and reliable networks at a low cost there are many more challenges to overcome. Mostly security and privacy challenges are categorized on the basis of their need, to overcome as quickly as possible. The most important challenges are as follows:

A. Object Identification

Objects are the building blocks of IoT that need to be identified physically or in the network [liv-lvi]. Sensor networks cover a huge area so adversaries can monitor the transmission between objects and gain access to the overall network. Without data integrity the overall naming structure of objects is insecure [xxx]. DNS cache positioning attacks can harm the overall working of the network. Object identification is important so each object can be uniquely identified. Fake objects should be identified as soon as possible as each object signifies potential spot of attack. The network must be protected from physical or logical attacks on devices and their data. **Identity Management:** The complex relation between interconnecting things possess security challenge to identify objects uniquely [xxviii, xxx].A proper object identification method is required to identify objects as well as reflecting all the important properties of the object. For these interconnecting objects identification of fake objects is most important. Many IoT devices don't have suitable user interfaces for communication to connect with each other [xxvii]. Therefore, a new device is needed with appropriate user interfaces for providing suitable communication between entities.

B. Authentication and Authorization

How to achieve authentication and authorization of objects? For unique identification of objects authentication and authorization can be achieved through ID passwords, cryptography and database based access control [xxx, xxxi, lvi, lvii]. Authentication can be achieved by cryptography algorithm. To provide secure communication between objects the interconnected devices need to verify themselves through trustable services. Many open research issues have been discussed for IoT objects' secure identification but a deeper research and analysis is necessity of the time. To uniquely identify all the “things” in IoTa more secure identity management is required.

C. Privacy

Due to the heterogeneity nature of the interconnected devices it has become difficult to accomplish user's privacy requirements [xxi, xxxi, xlviii, xlix]. Privacy is absolute human right which includes the control over personal information as well as what can be done with this information. It depends on the stakeholder to whom they want to share their personal information or not want to share at all. In IoT privacy is one of the most dominant challenges [xv]. Privacy Enhancing Technologies (PET) including VPN that provide better data integrity and confidentiality are new technologies for IoT devices [xxii, xxviii, xxx]. The privacy requirements for cloud coverage with IoT devices should also be considered. **Input privacy:** The input that users put should be kept private from everyone even from authorized receivers. The user data should be protected from the adversaries and attackers [xi]. **Output privacy:** The authorized receivers should be the only one that deciphered computation output and it should only give access to its authorized user. **Function privacy:** The underlying functions should be private and protected from attacker and unauthorized users. **Location Privacy:** Location privacy is the most critical as if it is disclosed it will disclose all the information of the user including user's personal living habits [xi, xvii, xviii]. The Pseudonyms technique is adopted here to hide user's location. However the location is not directly protected. The adversary can physically search most visited places of the user and can get access to information[xvii].

D. Network Security

Network security of interconnected things split into object confidentiality, object authenticity, object integrity, and object availability [xxviii, l, lviii]. Object confidentiality must be provided as it prevents sensitive information leakage on internet. Providing security to each layer increases complexity. Therefore, new Privacy Enhancing technologies (PET) have been developed for achieving these goals such as Virtual Private Networks (VPN), IPSec and Transport Layer Security (TLS). TLS connection is required for providing confidentiality and integrity. Authenticity provides proof of validity that claimed entity is the one that it claims to be. It provides secure connection with an authenticated entity. Integrity ensures that no data is lost or modified.

E. Identity Privacy

The fact of being the real user or claimed users refer to the identity privacy that should be well protected from public/attackers [xvii, xviii]. Sometimes, in emergency cases when some dispute occurs the privacy of information can also effect the scenario [xi]. Pseudonyms technique has been adopted to overcome this problem. The periodic updating of pseudonyms leads towards unbearable computational cost for IoT.

F. Trust

Trust is another crucial requirement of IoT due to its distributed nature. Maintaining trust in IoT is very important for its users. IoT must ensure sensing device's trust, entity trust, and data trust [xviii, xxx, xxxi]. Maintaining trust in the system for secure interaction between objects is important. IoT structure is facing challenges for providing trustable system to its users. IoT system must have decentralized models, implementation of new trust mechanisms and new applications maintaining trust for its users [xv]. Reputation management mechanisms will help to maintain the trust of objects in the network.

G. Removing or Adding Layers

To maximize rewarded credits sometimes social groups of IoT users remove the layers connecting them for forwarding this help them to reduce transmitters that are sharing the reward is called removing layer [xi]. To increase credits sometimes IoT users maliciously bypass the path of forwarding packets between them by increasing total obtainable utility and it is called adding layer [xi]. These attacks are dangerous for networks and can lead towards huge loss of the private information. We need better way of dealing with these attacks and provide quick solutions if something bad happen.

H. Forward and Backward Security

Another challenge is to provide forward and backward security in the network. The heterogeneous nature of IoT make it necessary to provide security and privacy for social formulated groups of users [xi]. It is necessary to provide backward and forward security for these users. The newly joined users must not have access to the mails before they join the network. Same goes for the users who left the network must not have access to the mails.

I. Lightweight Devices

Lightweight devices are another challenge as sensing objects are very small and contain lightweight processors that decrease the performance of network. Lightweight symmetric and asymmetric key management systems need to provide trustable services to the user [xv, lix]. Lightweight encryption and decryption algorithms should be used to provide security authentication [vi]. Designing lightweight security algorithms, protocols and their implementation is the key to tackle uncontrolled surrounding conditions of IoT network.

J. Object Compromise

Object compromise attack occur when some adversary attack the sensing device and extracts all the necessary and private information of the user as well as secret key [xi, xxxiv]. By gaining all the information they can reprogram or replace sensing IoT devices with malicious one that are under control of adversary. The adversary can select any object to attack and can damage the whole network.

IV. PROPOSED MODEL

Numerous sensors contribute from various hardware platforms for the exchange of information. IoT sensors engage people and communities in collecting data but managing data security and privacy with traditional techniques is a hard job. Current IoT devices are protected using traditional techniques that are prone to error. Many industries are using small sensing devices that are vulnerable to security theft and misuse of private data. Large scale implementation of sensing systems increases new challenges of privacy and security. Upon intensive review, it has been found that there is lack of any such model which can provide finest security system for small sensing devices of IoT. In this section, a model has been proposed (as shown in Fig. 3) namely Security Enabled Model (SEM) to overcome security and privacy challenges in IoT systems. Our proposed model detailed how small sensing devices can improve their applicability in real world scenario and eradicate the limitation of power consumption factor.

To illustrate the performance of the proposed model, it is assumed when the sensing devices generate data from diverse places then that data has to be visualized by end users. Hereafter, many end users request to view reports at the same time from server. These objects are concerned about three aspects of data: 1) Security and privacy mechanism 2) quick response and 3) data quality. The proposed model is comprised of three layers where each layer aims to provide security and privacy solutions and it also illustrates the sensing objects authentication and principles that IoT system should support.

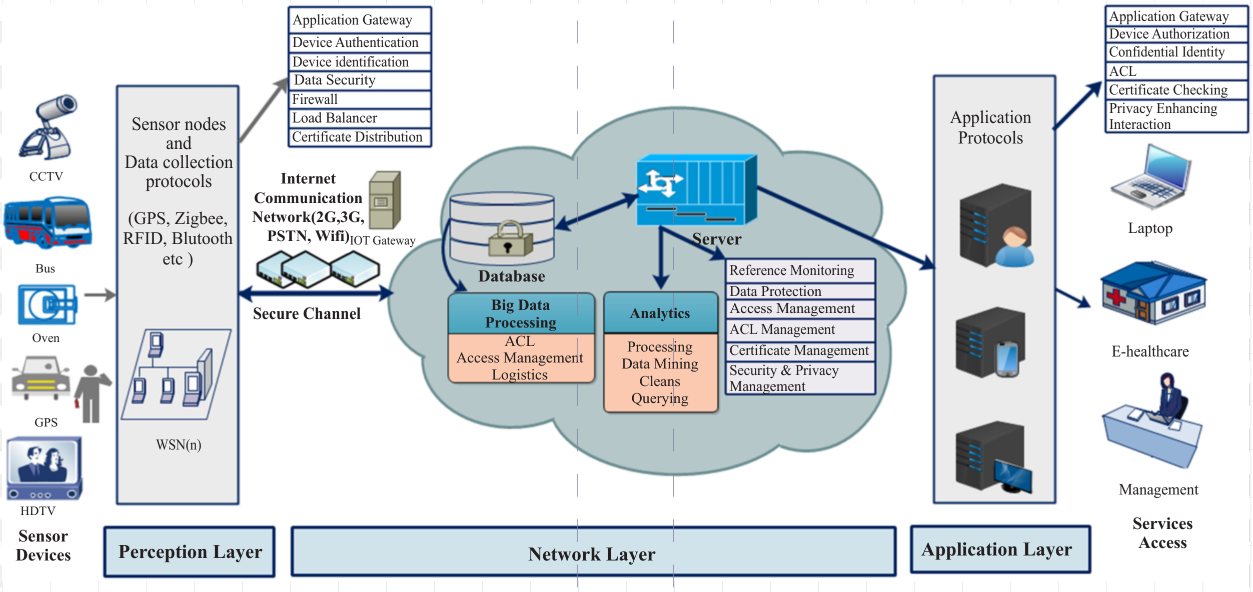

Fig. 3. Proposed Security Enabled Model (SEM) for IoT System

A. Perception Layer

Sensing devices collect data that is transmitted by using protocols e.g. Zigb towards the server system. The signals that carry data travel through public places so we need effective protection of data from being monitored and intercepted. Most sensing devices are installed in places where it can be easily accessed and monitored. The attacker can easily gain access to the equipment and can physically harm these devices. Currently, the most important security challenges of perception layer includes securing objects from being captured by unauthorized user, being secure from fake objects, protection from Denial of Service (DoS) attacks, protection from routing threats, timing and replay attack [xli]. We propose an authentication process through which sensing devices must be identified to make part of the network. Authentication process includes application Gateway for the checking of data sending sensors. Identification of fake object will become easy through checking the contents of sensing devices which they are sending. Firewall provides secure packet filtering that will enhance protection of data from internal and external networks. Load balancer and certificate distribution will enhance security as each device must have the certificate of being authorize and becoming part of the network. Through proposed authentication process the small sensors will be secure from unauthorized access to the device information. Further, this model will enhance the power of small sensing devices in order to make them more secure and smart.

B. Network Layer

When large number of objects sends data at the same time including fake objects, it can lead towards DoS attack in the network. Network layer security challenges include: reducing compatibility problems by providing data integrity and confidentiality, protecting privacy of user's, protection against DoS and Man in The Middle Attacks etc. [xxxi]. Existing internet security architecture is appropriate for the humans but IoT environment includes machines and humans so a new way of securing these devices is highly required. A new way of identifying objects is necessary as current IP technology cannot be applied on IoT. IoT system is facing challenges in the transmission of data that can be retrieved later. The data can be attacked during its transmission and at the time of retrieval. In this model, network layer transfers data to the cloud servers to process data where data is transferred by establishing secure channel to follow proposed authentication process through which each object is identified and their data contents are checked within the network. Furthermore, this layer includes cloud gateway that provides data driven Application Programming Interface (API) for collecting data from objects and route data to the servers for analysis. Cloud gateway safely transmits data from objects to servers for storage and data analytics that includes Access Control List (ACL) management. Server is the processing data center that will provide secure analytic services and server is also responsible for managing and evaluating reports, visualization, and querying data. Server maintains data and manages the ACL of each object's previous contributions. New analytical techniques support querying of data according to user requirements. Server maintains the status of each object and check the ACL for granting services to the users. Servers perform data mining techniques for knowledge discovery and real time analytics [xxxiv]. Data collected from diverse sources may be structured, unstructured or semi structured. We suggest a process for authentic access of database so that data may be accessed by authorized administrator and users only. For prevention of fraud in databases data mining techniques are implemented for fraud recognition. Preprocessing techniques of data are used for fraud recognition, validation, error modification and access control. Logistic regression is performed for managing the concurrency in the database. Managing data integrity constraints is the main challenge for specifying the uniqueness of data in database and it is well tackled in this proposed model.

C. *Application Layer*

Visualization is requested from end users to view reports of analysis and to get response of their queries. Data is managed from the start their will be no issue regarding processing of data. By using data delivery techniques and principles end users can visualize data that is authentic, secure, protected and according to the users standard. Data delivery techniques minimize latency, increase throughput of the system and provide faster retrieval of the data. The proposed model provides ACL for managing the access rights of each user. Only those who have certificate including the access list for interaction can gain access to services. Different applications have many complex security issues e.g giving reports to unauthorized person. In IoT environment it has become difficult to capture fake objects consequently new technologies are required for overcoming these situations. Application Layer Security challenges include authentication and restricting data access, dealing with large amount of data, providing data recovery and identity authentication. Sensing devices are sending data continuously so it becomes difficult to store massive amount of data. Therefore, protection of this massive amount of data is difficult. By following this process each object can have better privacy enhancing interaction and can gain services in a more secure way.

V. FUTURE DIRECTION\

As security and privacy issues are very serious concern that should be considered immediately. Since IoT technology deals with vast amount of personal and private data with the power of insure abilities to control its physical environment so significant solution for the security issues are required. The proposed model will protect physical and logical environment from any kind of theft and attacks. The smart devices that have embedded sensors will be identified for secure communication. However, new security technologies for the identification and data protection will be helpful in this regard. Designing new interfaces and security protocols for lightweight sensor devices in IoT network would be favorable and beneficial. Participants should also have knowledge and security privileges of the system. Future work also includes the deployment of proposed model in IoT based smart university and new security mechanism for lightweight IoT devices will also be targeted.

VI. CONCLUSION

IoT vision allows humans and machines to be connected with anything, anyone, anywhere and anytime. IoT devices can be part of any wireless sensor networks or wired networks simultaneously. Anyhow main concern of IoT is to create smart spaces like smart home, smart grid, smart transportation, smart traffic, smart cities and smart health for users. IoT concept is increasing speedily while facing different challenges; such as assuring availability and reliability, creating business models for interconnection of devices, security and privacy challenges for providing secure communication between devices. Intensive literature review has been conducted to identify and investigate various security and privacy challenges encountered by the IoT environment. Hence, security architecture has been designed to elaborate the current security and privacy challenges faced by IoT technology. Different challenges being faced by IoT layers have been identified in the current investigation. Moreover important security and privacy challenges were outlined like object identification, authentication, authorization, privacy, network security etc. Identification is the most important challenge as verifying fake objects for secure communication. This study proposed a Security Enabled Model (SEM) to cope with the outlined challenges and make IoT environment more secure and efficient. SEM ensures security at each layer of IoT moreover perception layer includes authentication process for the secure communication between sensors and Application Programming Interfaces (APIs). A part of authentication process is identification of objects and managing ACL for access rights, further it will provide better protection from malicious objects and manipulation of confidential data. Network layer that emphasis on data security so that data will be transferred from authentic objects through secure channel, moreover it will become easy for server to maintain security. Server also includes security process to manage unauthorized access through reference monitor. At the end application layer includes visualization of data to provide services to its intended users. To sum up, it was identified that data will be collected from secure objects which lead towards a secure network communication by using firewall and load balancer. Transferring data from secure objects towards server that includes secure database for the storage and analytics is another feature of this model. Server manages reference monitors and certifies authorities. Eventually, passing from secure server towards end users, data will be protected by implementing this model. Besides, in order to create most secure IoT environment we need more encryption algorithms and their implementation. Only authorized users can get the desired services through the proposed model.

REFERENCES

[i] H. Chan and A. Perrig, "Security and Privacy in Sensors Networks". Computers, 36(10): p. 103-105. 2003.

[ii] J. B. Gubbi, R. Marusic, S. Palaniswami and Marimuthu, "*Internet of Things (IoT): A vision, architectural elements, and future directions.*" Future generation computer systems, 2013. 29(7): p. 1645-1660.

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

[iv] R. Roman, P. Najera and J. Lopez, "*Securing the internet of things.*" Computer, 2011. 44(9): p. 51-58.

[v] S. Haller, S. Karnouskos and C. Schroth, "*The internet of things in an enterprise context.*" Future Internet Symposium. 2008. Springer.

[vi] A. F. Skarmeta, J. L. H. Ramos and M. V. Moreno, "*A decentralized approach for security and privacy challenges in the internet of things.*" Internet of Things (WF-IoT), 2014 IEEE World Forum on. 2014. IEEE.

[vii] F. Tao, Y. Zuo, L. D. Xu and L. Zhang, "*IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing.*"IEEE Transactions on Industrial Informatics, 2014. 10(2): p. 1547-1557.

[viii] S. D. T. Kelly, N.K. Suryadevara and S. C. Mukhopadhyay, "*Towards the implementation of IoT for environmental condition monitoring in homes.*"IEEE Sensors Journal, 2013. 13(10): p. 3846-3853.

[ix] K. D. Chang, C. Y. Chang, H. M. Liao, J. L. Chen and H. C. Chao, "*A Framework for IoT objects management based on future internet IoT-IMS communication platform.*" Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013. IEEE.

[x] M. Aazam, I. Khan, A. A. Alsaffar and E. N. Hu,"*Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved.*" 11th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2014. 2014. IEEE.

[xi] J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "*Security and privacy for cloud-based IoT: challenges.*" IEEE Communications Magazine, 2017. 55(1): p. 26-33.

[xii] D. Bandyopadhyay, and J. Sen, "*Internet of things: Applications and challenges in technology and standardization.*" Wireless Personal Communications, 2011.58(1): p. 49-69.

[xiii] B. Dorsemaine, J. P. Gaulier, J. P. Wary, N. Khier and P. Urien,"*Internet of Things: a definition & taxonomy.*"9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015. 2015. IEEE.

[xiv] T. Xu, J. B. Wendtand M. Potkonjak,"*Security of IoT systems: Design challenges and opportunities.*" Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design. 2014. IEEE Press.

[xv] M. Abomhara, and G. M. Køien, "*Security and privacy in the Internet of Things: Current status and open issues.*" International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014. 2014. IEEE.

[xvi] E. Bertino, "*Data Security and Privacy in the IoT.*" EDBT. 2016.

[xvii] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. A. Savikko, H. Leppakoski, M. Z. H. Bhuiyan, S. B. Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari and H. Kuusniemi, "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey". IEEE Access, 2017.

[xviii] J. Daubert, A. Wiesmaier and P. Kikiras, "*A view on privacy & trust in IoT.*"IEEE International Conference on Communication Workshop (ICCW), 2015. 2015. IEEE.

[xix] J. P. Hubaux, S. Capkun and J. Luo, "*The security and privacy of smart vehicles.*" IEEE Security & Privacy, 2004. 2(3): p. 49-55.

[xx] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "*Security of the internet of things: Perspectives and challenges.*" Wireless Networks, 2014. 20(8): p. 2481-2501.

[xxi] P. McDaniel, and S. McLaughlin, "*Security and privacy challenges in the smart grid.*" IEEE Security & Privacy, 2009. 7(3).

[xxii] S. Nath, and S. Som, "*Security and Privacy Challenges: Internet of Things.*" Indian Journal of Science and Technology, 2017. 10(3).

[xxiii] C. C. Niu, K. C. Zou, Y. L. O. Yang, G. J. Tang and Y. Zou,"*Security and Privacy Issues of the*

Internet of Things." Applied Mechanics and Materials. 2013. Trans Tech Publ.

[xxiv] H. K. Patil, and R. Seshadri, "*Big data security and privacy issues in healthcare*." Big Data (BigData Congress), 2014 IEEE International Congress on. 2014. IEEE.

[xxv] H. C. Pöhls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. D. Rodriguez, and T. Mouroutis,"*RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects*." IEEE. Wireless Communications and Networking Conference Workshops (WCNCW), IEEE. 2014.

[xxvi] K. A. Rafidha Rehiman and D. S.Veni, "*Security, Privacy and Trust for Smart Mobile devicesin Internet of Things – A Literature Study*." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)2015. 4.

[xxvii]A. R. Sadeghi, C. Wachsmann, and M. Waidner, "*Security and privacy challenges in industrial internet of things*." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/ IEEE. 2015. IEEE.

[xxviii]E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier and P. Kikiras,"*On the Security and Privacy of Internet of Things Architectures and Systems*." *International Workshop onSecure Internet of Things (SIoT),* 2015. IEEE.

[xxix] R. H. Weber, "*Internet of Things–New security and privacy challenges*." Computer law & security review, 2010. 26(1): p. 23-30.

[xxx] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen and S. Shieh,"*IoT security: ongoing challenges and research opportunities*." IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA), 2014. IEEE.

[xxxi] K. Zhao and L. Ge, "*A survey on the internet of things security*." *International Conference on Computational Intelligence and Security (CIS), 2013 9th*. 2013. IEEE.

[xxxii]M. Dabbagh, and A. Rayes, "*Internet of Things Security and Privacy.* Internet of Things From Hype to Reality. 2017, Springer. p. 195-223.

[xxxiii]L. Tan, and N. Wang, "*Future internet: The internet of things*."3rd International Conference *on*Advanced Computer Theory and Engineering (ICACTE). 2010. IEEE.

[xxxiv]A. Karim, A. Siddiqa, Z. Safdar, M. Razzaq, S. A. Gillani, H. Tahir, S. Kiran, E. Ahmad and M. Imran, "*Big data management in participatory sensing: Issues, trends and future directions*." Future Generation Computer Systems, 2017.

[xxxv]F. Xia, L. T. Yang, L. Wang and A. Vinel, "*Internet of things*." International Journal of Communication Systems, 2012. 25(9): p. 1101.

[xxxvi]H. Kopetz, "*Internet of things*, in *Real-time systems*."2011, Springer. p. 307-323.

[xxxvii]F. Wortmann and K. Flüchter, "*Internet of things*." Business & Information Systems Engineering, 2015. 57(3): p. 221-224.

[xxxviii]L. Atzori, A. Iera, and G. Morabito, "*The internet of things: A survey*."Computer networks, 2010. 54(15): p. 2787-2805.

[xxxix]S. H. Yang, "*Internet of things*."Wireless Sensor Networks". 2014, Springer. p. 247-261.

[xl] G. M. Lee, N. Crespi, J. K. Choi and M. Boussard, "*Internet of things*." Evolution of Telecommunication Services. 2013, Springer. p. 257-282.

[xli] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin,"*Iot gateway: Bridging Wireless sensor networks into internet of things*."2010 IEEE/IFIP 8th International Conference onEmbedded and Ubiquitous Computing (EUC), 2010. IEEE.

[xlii] F. Bonomi, R. Milito, J. Zhu, S. Addepalli"*Fog computing and its role in the internet of things*." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. 2012. ACM.

[xliii] E. Baccarelli, P. G. V. Naranjo, M. Scarpiniti, M. Shojafar and J. H. Abawajy,"*Fog of Everything: Energy-efficient Networked Computing Architectures, Research Challenges, and a Case Study*."IEEE Access, 2017.

[xliv] H. Suo, J. Wan, C. Zou and J. Liu"*Security in the internet of things: a review*." International Conference onComputer Science and Electronics Engineering (ICCSEE), 2012. IEEE.

[xlv] D. Miorandi, S. Sicari, F. D. Pellegrini and I. Chlamtac, "*Internet of things: Vision, applications and research challenges*." Ad Hoc Networks, 2012. 10(7): p. 1497-1516.

[xlvi] Y. K. Chen, "*Challenges and opportunities of internet of things*." 17th Asia and South Pacific, Design Automation Conference (ASP-DAC), 2012 2012. IEEE.

[xlvii] J. Schrammel, C. Hochleitner and M. Tscheligi, "*Privacy, trust and interaction in the internet of things*." *International Joint Conference on Ambient Intelligence*. 2011. Springer.

[xlviii]A. S. Ukil, S. Bandyopadhyay and A. Pal, "*Iot-privacy: To be private or not to be private*."IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*,* 2014. IEEE.

[xlix] C. Perera, R. Ranjan, L. Wang, S. U. Khan and A. Y. Zomaya, "*Privacy of big data in the internet of things era*." IEEE IT Special Issue Internet of Anything, 2015. 6.

[l] C. M. Medaglia, and A. Serbanati, "*An overview of privacy and security issues in the internet of things*."The Internet of Things. 2010, Springer.

p. 389-395.

[li] J. H. Ziegeldorf, O. G. Morchon and K. Wehrle, "*Privacy in the Internet of Things: threats and challenges*." Security and Communication Networks, 2014. 7(12): p. 2728-2742.

[lii] F. T. Commission, "*Internet of Things: Privacy & security in a connected world*." Washington, DC: Federal Trade Commission, 2015.

[liii] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila and A. Vasilakos, "*The quest for privacy in the internet of things*." IEEE Cloud Computing, 2016. 3(2): p. 36-45.

[liv] D. Uckelmann, M. Harrison and F. Michahelles, "*An architectural approach towards the future internet of things*." Architecting the internet of things. 2011, Springer. p. 1-24.

[lv] M. Kranz, P. Holleis and A. Schmidt, "*Embedded interaction: Interacting with the internet of things*." IEEE internet computing, 2010. 14(2): p. 46-53.

[lvi] X. Jia, Q. Feng, T. Fan and Q. Lei,"*RFID technology and its applications in Internet of Things (IoT)*." 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012. IEEE.

[lvii] J. Liu, Y. Xiao and C.P. Chen, "*Authentication and access control in the internet of things*."32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2012. IEEE.

[lviii] L. Atzori, A. Iera, G. Morabito and M. nitti, "*The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization*." Computer networks, 2012. 56(16): p. 3594-3608.

[lix] J. Y. Lee, W.C. Lin, and Y. H. Huang, "*A lightweight authentication protocol for internet of things*." International Symposium on Next-Generation Electronics (ISNE), 2014. 2014. IEEE.