JFSA

Journal of Futuristic Sciences and Applications
Vol. 5(2), Jul-Dec 2022, pp. 54-64
doi: 10.51976/jfsa.522208
www.gla.ac.in/journals/jfsa

Proposed Model in IoT Security Layer for Ethical Security Management

*Neeraj Kumar Pandey**

ABSTRACT

With the number of similar applications and concepts being used these days the threats of cyber-attacks are also high, where completely different attacks and threats can result in serious problems to the whole system of the network, hence making the concepts of security system to be extremely important. The present analysis helps in discussing the management of security in IoT networks discussing it in five sections. We tend to 1st illustrate the background and conception behind the idea of IoT. After which the needs for safety for IoT are mentioned. In the next section, the projected design may be wont to return up with safety management has been elaborated. Then we tend to implement web protocol security because of the Network Cryptography system security. An example of however handily this projected design may be wont to return with proper management of safety for the IoT network was also explained intimately.

Keywords: *IoT; Security and management; Threats and attacks; Design and layers; Network security; Science security; Cryptography.*

1.0 Introduction

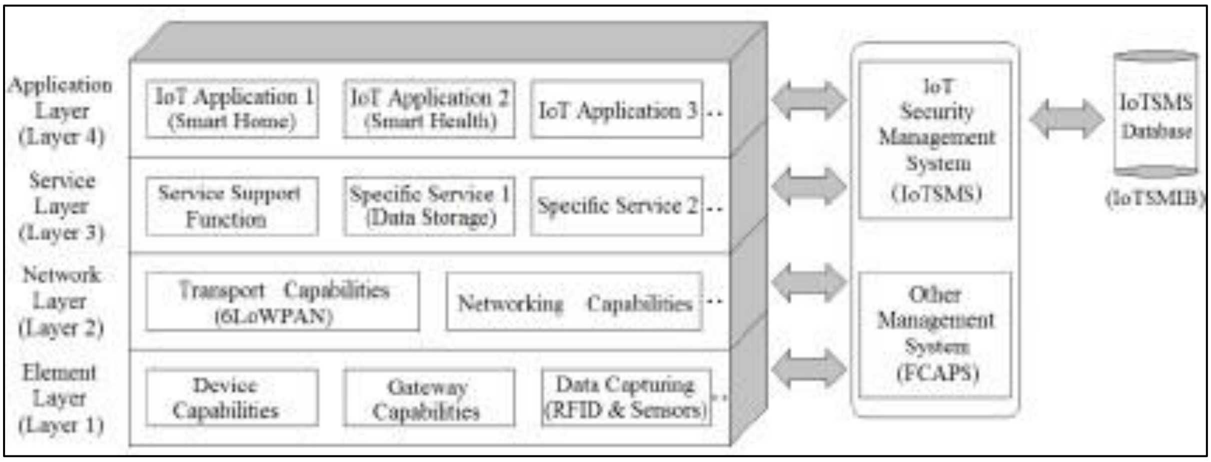
The architecture of the IoT network infrastructure could endorse the IoT safety management system (IoT-SMS). There are 5 specific security concerns within the IoT network structure in square measure; every one of the network is considered before preparing with a system of security management such protection concerns calculate that good square sensors measure simple to assault, security monitoring can help good low-power systems, privacy issues with part layer devices, entirely separate layers face similar risks, and problems with system compatibility and complexity [1]-[5]. These specifications mean that we would like to build an IoT eco- system protection monitoring framework that counters all potential risks and is compliant with the IoT specification. In other words, because the IoT network environment is intended as four-layer device architecture, the network security management should be structured as a bedded framework on equal lines. [6] [7] We prefer to suggest a four-layer protection management scheme for the IoT ecosystem to incorporate this concept, much like that used for the functional nature of IPsec. There are four functional levels of the projected IoT protection management framework (IoT-SMS). The concepts that were implemented to establish four square measurement layers were as follows, a layer of practicality is formed wherever differentia special unique distinct} kind of security functions on a different level is required. Each layer conducts well-defined safety activities. For current uniform protocols, the practicality of each layer is considerably selected. To decrease the info flow through the device interfaces, the layer boundaries are selected.

**Assistant Professor, School of Computing, DIT University, Dehradun, Uttarakhand, India*
(E-mail: dr.neerajkpandey@gmail.com)

The number of layers is consistent with the layers of the IoT framework in such a manner that separate protection tasks do not need to be executed inside the same layer.

2.0 IoT Layers Reference Model

Figure 1: The IoT Layered Reference Model


Application Layer (Layer 4)
Service Layer (Layer 3)
Network Layer (Layer 2)
Element Layer (Layer 1)
IoT Application 1 (Smart Home)
IoT Application 2 (Smart Health)
IoT Application 3
Service Support Function
Specific Service 1 (Data Storage)
Specific Service 2
Transport Capabilities (6LoWPAN)
Networking Capabilities
Device Capabilities
Gateway Capabilities
Data Capturing (RFID & Sensors)
IoT Security Management System (IoTSMS)
Other Management System (FCAPS)
IoTSMS Database
(IoTSMIB)

2.1 IoT layered architecture

The materials, coordination principles, and protocols of each layer are detailed below. The benefits of the stratified design are:

- Providing the IoT with standard management. To improve the general safety of the IoT network infrastructure, we will enforce numerous security protocols, security services frame- works at any layer [8].
- The stratified system is extensible, which is why the lower area unit receives higher layer facilities.
- Allowing the latest technology integration into a prevalent IoT network infrastructure for each hardware and software system, and therefore the stratified structure is simple to handle in a rather sensible deployment still as a portion [9].

2.1.1 Element layer

The component layer is lowest IoT layer. It is the system layer and comprises different node and sensor types, like the RFID, actuators, barcode labels, and smart detection systems. Be- sides, these square measurement sensors cannot evaluate the artifacts while they move the collected information to the future layer. Modules accumulate information and pass it to the network layer [10].

2.1.2 Network layer

The network layer is responsible of transmitting the data to the higher layer the information obtained from the component layer. Network layer helps in transmitting knowledge to the higher layer through component layer. Through the prevalent communication methods, the network layer transmits information either through a wireless or wired network, cloud, inter- net, satellite network, cell network, or military network. An IoT asks for measurability [11].

2.1.3 Service layer

It consists of features that process the knowledge gathered and provide storage links for the knowledge gained from the component layer. The IoT layer serves as an interface of the associate degree between the various IoT devices and provides communication methods be- tween the weather. A property between sensors is provided by the service layer on the top of the network layer. It also offers services to ensure efficient, purposeful communication be- tween apps and devices. For the associate degree RFID device, is an associate degree example of a service layer, we will mention the “Open Remote” as an associate degree example of a service layer implementation, like the middleware response for business and residential buildings and automation [12].

2.1.4 Application layer

The platform layer consists of a spread of IoT smart software that has supported consumer requirements. The application layer utilizes many different protocols, CoAP, the MQTT, the AMQP, and XMPP. [13]

2.1.5 Data flow between layers

The IoT data flow can be broken into 4 stages: information assortment, transfer of knowledge, preservation of knowledge, and review of knowledge. Fault, setup, accounting, efficiency, and protection management functions are necessary for the information assortment and storage to execute the supposed 5 familiar network management (FCAPS) functions [14].

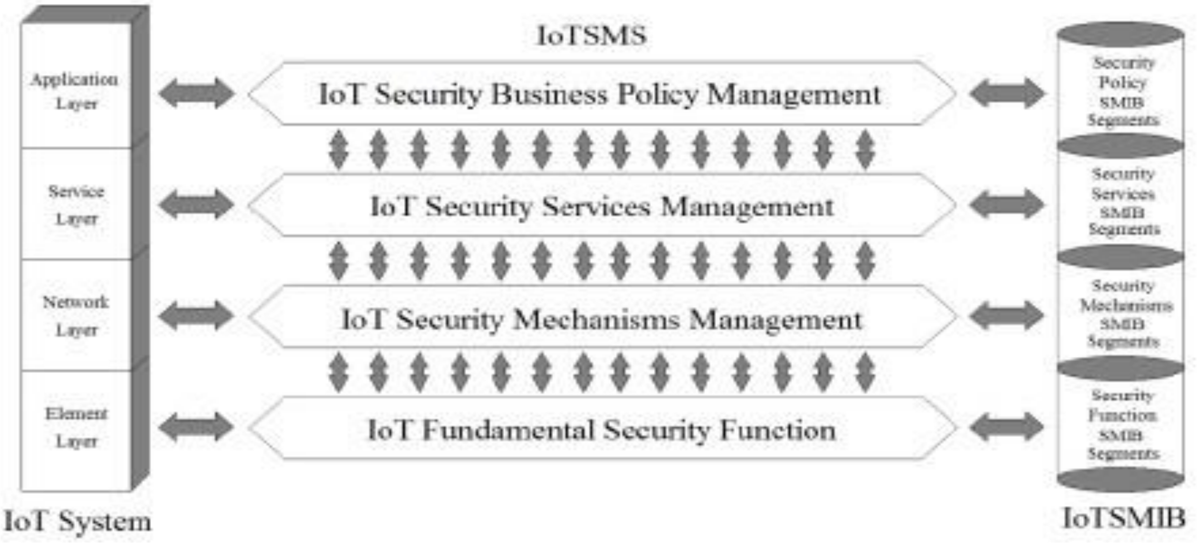
3.0 IoT Security Layer (Proposed Model)

The billions of good devices can produce a Brobdingnag Ian quantity of information daily. This information is wont to deliver a higher the user’s expertise, up the product services, and profit the event of the empirical search like business management, automatic driving, health, and fitness. Our lives have been modified by the net. [15] The IoT is now absorbing our everyday lives, but a lot of the general public discourse about whether or not to just embrace or condemn the IoT includes protection concerns. Key of this study is to further deliver security purposeful design as simple security management of IoT methods to meet the needs of end- users and network providers. Security control systems for the IoT to address the demands of end consumers and network operators. IoT protection management can provide information protection from the very cheapest to highest layers of IoT; the different security policies, mechanisms and services, firmly protect helpful data privacy information. [16]

3.1 IoT security management system

There are 3 parts of the architecture for security management; the design of the IoT network structure consisting of 4 layers on left has been demonstrated. IoTSMS is in middle half, which has four levels of defense business plan management, IoT security services management, elementary IoT security efficiency and also IoT security system management. Like pseudorandom generator, mutual, regular arithmetic output, etc., every layer with its necessary practicality in protection management to provide secrecy of information, the credibility of information, and usability of the information. On the right side of the diagram, the SMIB applies the X.509 version three recommendation authentication, among, the IoT protection management database (SMIB).

Figure 2: Security Management System for IoT


IoTSMS
Application Layer
Service Layer
Network Layer
Element Layer
IoT System
IoT Security Business Policy Management
IoT Security Services Management
IoT Security Mechanisms Management
IoT Fundamental Security Function
Security Policy SMIB Segments
Security Services SMIB Segments
Security Mechanisms SMIB Segments
Security Function SMIB Segments
IoTSMIB

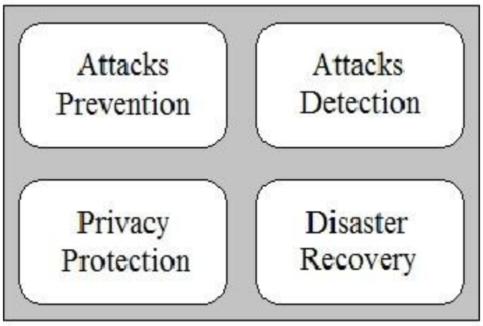
3.2 Functional layers of security management for IoT

As stated before, the square tests four levels of IoT protection control. They are the management layer of IoT security corporate strategy, the management layer of IoT military intelligence, the management layer of IoT security mechanisms, and the operational layer of elementary IoT security. Each layer has its activities to protect the IoT security management framework. [8]

3.2.1 Requirements of IoT security business policy management

The security business decision management layer is concerned with the business customer's wishes, such as interference and stopping all risks from attacks for very different purposes, retaining the privacy of all successful computers, protecting the IoT infrastructure from at- tacks, and preventing system failure.

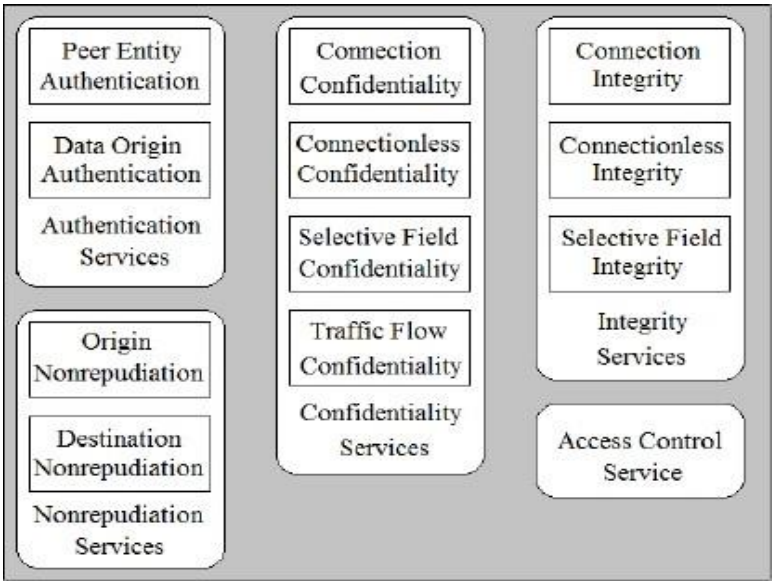
Figure 3: IoT Security Business Policy Management Requirements



3.2.2 IoT security services function

The most important security services such as authentication services along with peer agency and data root authentication are included in the useful layer component of IoT defense services. Confidentiality can be the most popular IoT security facet, such as confidentiality, selective filed confidentiality. The knowledge inside the IoT environment is continually dynamic. Service of dignity during this atmosphere suggests that only approved mechanisms can make improvements. Integrity services are important for the protection of the IoT systems, along with relationship integrity, connectionless integrity, and selective filed integrity, non-repudiation services along with origin non-repudiation and destination non-repudiation, and even access management program.

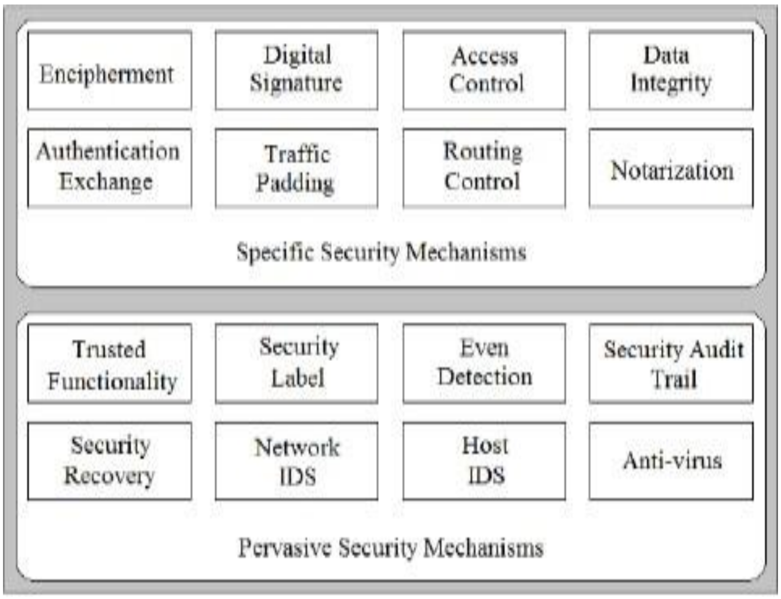
Figure 4: IoT Security Services Functionality Layer


Peer Entity Authentication
Data Origin Authentication
Authentication Services
Origin Nonrepudiation
Destination Nonrepudiation
Nonrepudiation Services
Connection Confidentiality
Connectionless Confidentiality
Selective Field Confidentiality
Traffic Flow Confidentiality
Confidentiality Services
Connection Integrity
Connectionless Integrity
Selective Field Integrity
Integrity Services
Access Control Service

3.2.3 IoT security mechanism function

Security structures have the required procedures, algorithmic rules, and schemes to enable those security services described within the layer of security services.

Figure 5: IoT Functionality Mechanisms Layer

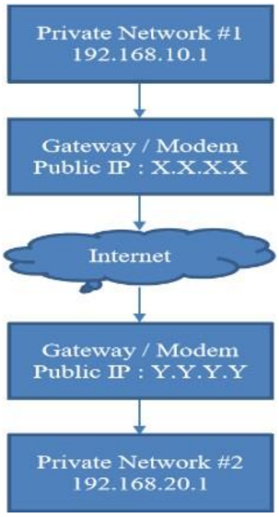


The layer of the practicality of the IoT protection framework provides the security mechanisms or ubiquitous mechanisms. Precise protection measures include decryption, digital signatures, access control, the integrity of information, sharing of identification, traffic objects, routing management, and security mechanisms for notarization. Sure practicality, security mark, also identification, security audit route, network, host IDS, anti-virus security and security recovery mechanisms were included in the widespread security mechanisms.

3.2.4 IP security implementation

The packet data and headers to be sent are being computed using cryptographic checksum techniques and change the IP packet header section using a secure hashing function in tunnel mode. It adds a new header containing the hash value so that the information provided in the normal package is authenticated in the recipient. It seems to create a special tunnel on a public network that is only accessible to a range of people. The below figure illustrated the example of an IP Security usage diagram for building secure communications using public networks.

Figure 6: IP Security Implementation [11]

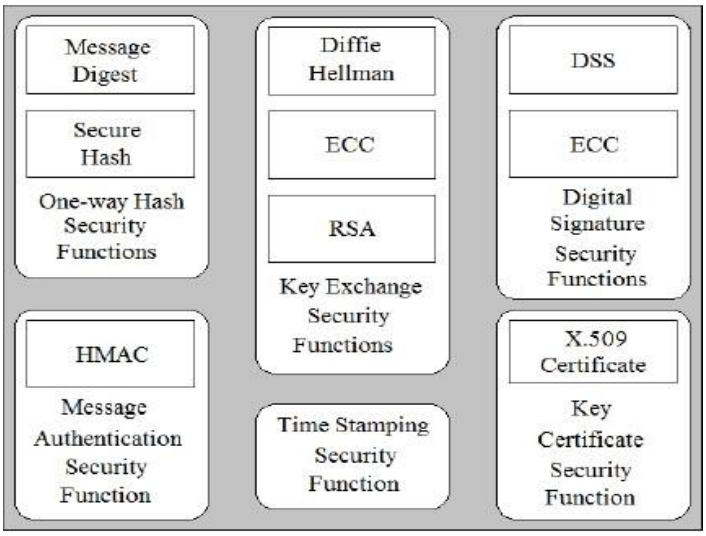


The private network #1 and #2 uses the local IP addresses, 192.168.10.1, and 192.168.20.1. Both gateways use public IP, and they can be easily accessed from any computer as long as they are connected to the internet. There are a few steps to connect from internal network #1 to #2. Every packet sent to IP 192.168.20.1 must be wrapped into another packet so that the IP header that appears is public IP X.X.X.X Then it will be sent to public IP Y.Y.Y.Y through a gateway with IP header stating as if the packet came from IP X.X.X.X. The process is called encapsulation. The gateway must know the path to achieve IP 192.168.20.1. It must redirect the packet to IP 192.168.20.1. It creates a special tunnel between the two networks. Once the connection has been established, each network can communicate and ping. When the packets arriving at IP Y.Y.Y.Y, they must be encapsulated to obtain the actual packet and sent to IP address 192.168.20.1 [11]

3.2.5 Fundamental IoT security function

An elementary feature of the SMS IoT was used in an autonomous comprehensive server of the security because it might give better security to more than one application in a similar time. Hence, a very cheap practicality layer was taken into account to incorporate numerous generic cryptography and arithmetic modules. An IoT elementary security offers fundamental functions of security like the message digest, unidirectional hash, as well as the algorithms of secure hash. The functions of key exchange security together with an elliptic curve, Diffiedramatist, and RSA algorithms area unit together in the layer. Timestamping, certificates, authentication code, message authentication, elliptic curve algorithms, as well as the Digital signature normal together with the X.509 certificate normal is enclosed. The layer was comprised of all needed cryptologic functions for the Internet of Things SMS to work.

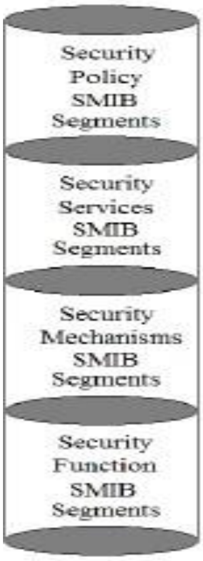
Figure 7: Fundamental Security Functionality Layer


Message Digest
Secure Hash
One-way Hash Security Functions
Diffie Hellman
ECC
RSA
Key Exchange Security Functions
DSS
ECC
Digital Signature Security Functions
HMAC
Message Authentication Security Function
Time Stamping Security Function
X.509 Certificate
Key Certificate Security Function

3.3 IoT security management information base

A critical aspect of the IoT SMIB is the IoT SMIB. This knowledge can be designed to facilitate the application of all IoT protection services in a very computational framework or contact environment. The IoT Protection Management Info Base is the abstract component of critical sensor IDs, user accounts, and security logs, and access management lists. [12]

Figure 8: The IoT SMIB Segment


Security Policy SMIB Segments
Security Services SMIB Segments
Security Mechanisms SMIB Segments
Security Function SMIB Segments

3.4 PKI for the IoT Security

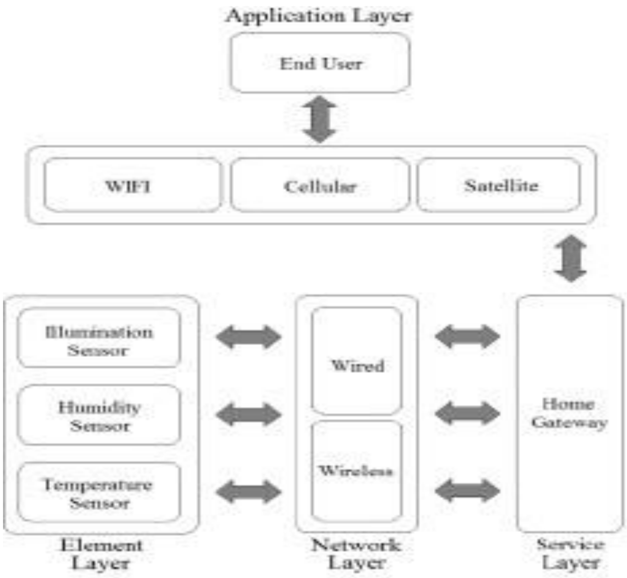
The General Public Key Infrastructure (PKI) was developed by the Engineering Task Force (IETF) to establish a confidence paradigm for many. [14] As much as the protection of the IoT framework matters, the critical output of PKI is supplying X.509 keys, key storage, and upgrading, delivering services to certain protocols, and providing access control. PKI offers a simple mechanism for data protection by malicious coding and authentication in communications. The IoT device is not vulnerable to brute-force and destructive attacks as it has PKI in situ. PKI guarantees the integrity of the data gathered by the sensors and nice devices and offers access to the protocol and program setup that is still convenient. PKI also maintains that the portion layer remains confidential inside the IoT framework. PKI offers a mix of mathematically related public-private keys. If the information is used to encrypt one key, the information can only be decoded by the opposite associated key. The knowledge gathered by the sensors and successful devices is protected using a public key in the case of the component layer inside the IoT framework, therefore the non-public key to decipher is mistreated.

3.5 Advantages of the modular security management system for IoT

The IoT protection management architecture offers a standard structure with a plurality of security resources and a plurality of frameworks for security monitoring. Therefore, the introduction of protection standards for vendors, network suppliers, and producers of products. Through introducing the economical elementary protection operation, numerous Security Service management modules can invoke separate security framework modules to assess the optimal security needs and management of the IoT network framework. The IoT-SMS standard protection management system integrates cost-effective monitoring methods and processes within the IoT network system, assisted by the security requirements of consumers. The expected IoT-SMS, as emerging methods and technology, would also accommodate new protection. It offers a regular protection framework in the setting of the Nursing IoT device Associate

3.6 An IoT security management scenario

Figure 9: Concept of the Smart Home Scenario



Look into a sensible scenario for home protection management. The owner of the house wants to observe the standard of comfort in his house. [13] The owner of the property, however, is at its geographical point and requires to use his/her mobile to observe the weather, wetness in his/her house as well as lighting.

3.7 Protocols used in the IoT SMS scenario

We prefer to use the wireless networking protocol IEEE 802.15.4 to include the required protection services of anonymity, authentication, and honesty to satisfy the specifications of low-power and low-speed sensitive devices inside the component layer. We prefer to use the 6LoPWAN protocol at the network layer, which introduces the process of low-power and lossy network routing. The routing system incorporates AES for a raincoat with 128-bit keys and supports RSA for digital signatures with SHA-256 to provide secrecy and reputation protection services. We prefer to use the CoAP protocol that runs over the UDP in the application layer to reduce the specifications for information estimation and resource-constrained systems and devices with low power consumption. The CoAP protocol offers a contact paradigm of "request and response" between the endpoints and adopts the AES because of the cryptological formula to supply the aforementioned protection services.

Figure 10: Protocols Used in the Smart Home

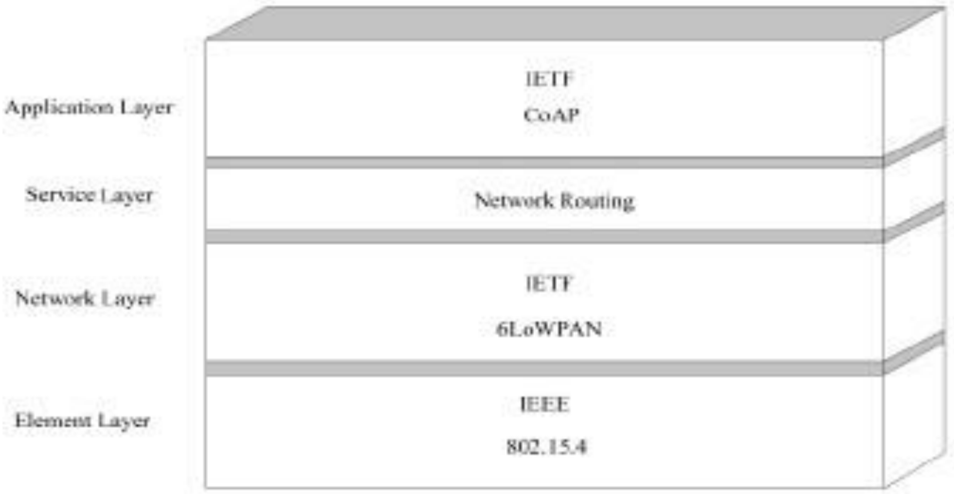


Table 1: Comparison of Existing Security Protocols in the Smart Home Scenario

Layers	**Protocols**		**Security Services**		
Element Layer	IEEE 802.15.4	Confidentiality	Authentication	Integrity	Access Control
Network Layer	IETF 6 LoWPA N	Confidentiality	Authentication	Integrity	Availability
Service Layer	IEEE Routing	Confidentiality	Authentication	Integrity	Key Management
Application Layer	IETF CoAP	Confidentiality	Authentication	Integrity	Non-Repudiation

3.8 Data flow by the smart home scenario [15]

Different sensors capture the information of surrounding data like vapor concentration, temperature, and lightweight pressure. Then the data is processed to form a digital signature message by a unidirectional hash that is invoked inside the component layer by an authentic module of service management. The AES symmetric-key crypto implements the IEEE 802.15.4 protocol. The understanding which comes from component layer is encrypted mistreatment that the standard hidden writing runs, invoked inside the network layer by the module for identity integrity service management. The 6LoWPAN protocol incorporates the routing system of low-power and lossy networks that makes use of AES with 128-bit keys that provide secrecy and authentication services for integrity [14] [15]. The encrypted information was obtained by the service layer and even the accessibility service management module invokes the operating module of the "Network Intrusion Detection System" (NIDS) to avoid the DoS assault in the transmission through internet, local area network, or cellular network. To validate the identification of the customer through inspection of the user profile, the authentic framework of service management inside the application layer invokes the main certification authority module. Then, the consumer decrypts the private key that the PKI module uses for the message victimization. "The CoAP protocol offers a coordination model for "request and answer" between the end-points. The consumer can use the API appliance on a good phone to remotely observe the temperature, humidity as lighting inside the house under the economic security safety

4.0 Conclusion

An important aspect of this analysis is to deliver a total security useful design yet as terribly straightforward security management strategies of an IoT network to fulfil every requirement of the users for the network suppliers. The science security protocol is within the network layer the protection management system of the web of Things may protect of (the information the info the data) from lowest layers to higher most layers of IoT network demanded privacy and data information were also protected firmly by different services, mechanisms and policies.

Reference

[1] Ovidiu Vermesan, Peter Friess, net Of Things: connection Technologies for Smart environments And Integrated system. Aalborg, Denmark: watercourse Publishers, 2013.

[2] Ovidiu Vermesan, Peter Friess, net Of Things from Analysis and Innovation to Market Deployment. Aalborg, Denmark: watercourse Publishers, 2014.

[3] Klaus Finkenzeller, Rfid enchiridion elementary And Applications in Contactless Smartcards, frequency Identification, And Near field Communication. Wiltshire, UK: John Wiley & Sons, 3RD Ed., 2010.

[4] Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "A Survey of bea- con-enabled Ieee 802.15.4 Mack Protocol in Wireless detector Networks," Ieee Communication Survey& Tutorials, Vol. 16, Pp. 856-876, Dec 2013.

[5] Saniya Vohra, Rohit Srivastava, “A Survey on Techniques for Securing 6LOWPAN,” Fifth International Conference on Communication Systems and Net- work Technologies, Pp. 643-646, April 2015.

[6] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Christ Alonso-Zarate, “A Survey on Application Layer Protocols For the web Of Things,” group action On IoT and Cloud Computing, Pp. 1-8, April 2015.

[7] Davide Conzon, Thomas Bolognesi, Paolo Brizzi, Antonio Lotito, Riccardo To- masi, Maurizio A. Spirito, “An Xmpp primarily based design For Secure IoT Com- munications,” Interational Conference On pc Commination’s and Networks, Pp. 1- 6, August 2012.

[8] H. Alshamrani, “Internet Protocol Security (IPsec) Mechanisms,” International Journal of Scientific & Engineering analysis, Vol. 5, No. 5, pp. 85-87, 2014.

[9] P. K. Singh and P. P. Singh, “A Novel Approach for the Analysis & problems with IPsec Vpn,” International Journal of Science and analysis, Vol. 2, No. 7, pp. 187- 189, 2013.

[10] A. Singh and M. Gahlawat, “Internet Protocol Security (IPsec),” International Jour- nal of pc Networks and Wireless Communications, Vol. 2, No. 6, pp. 717-721, 2012.

[11] HareKrishna Kumar and V.K. Tomar. “Stability analysis of sub-threshold 6T SRAM cell at 45 nm for IoT application” International Journal of Recent Technol- ogy and Engineering (IJRTE), 8(2):2432-2438, July 2019.

[12] T. Sharma and S. Shiwani, “Statistical Results of IPsec in Ipv6 Networks,” Inter- national Journal of pc Applications, Vol. 79, No. 2, pp. 15-19, 2013.

[13] Nira, Shukla A. (2021) Optimal Multiple Access Scheme for 5G and Beyond Communication Network. In: Senjyu T., Mahalle P.N., Perumal T., Joshi A. (eds) In- formation and Communication Technology for Intelligent Systems. ICTIS 2020. Smart Innovation, Systems and Technologies, vol 195. Springer, Singapore. https://doi.org/10.1007/978-981-15-7078-0_5

[14] R. Rahim and A. Ikhwan, “Study of 3 Pass Protocol on Information Security,” In- ternational Journal of Science and analysis, Vol. 5, No. 11, pp. 102104, 2016.

[15] A. Lubis And A. P. U. S., “Network forensic Application normally Cases,” Iosr Journal Of pc Engineering, Vol. 18, No. 6, pp. 41-44, 2016

[16] Punit Gupta, Jasmeet Chhabra, “ It primarily based good Home-style exploitation Power and Security management,” International Conference on Innovation and Challenging in Cyber Security, Pp. 6-10, August 2016.