www.rsya.org

Journal of Analytical Research

Vol 3 – Issue 2, Jul-Dec 2023
www.rsya.org/jar

ISSN: 2584-0037

Ethical Security Management Proposed Model in the IoT Security Layer

Prakash Singh Pundhir[1], Rahees Khan[2,*]

[1]Department of Computer Science and Engineering, GLA University Mathura, India 281406
[2]Department of Computer Science and Engineering, Aligarh Muslim University, Aligarh, 202002, India
[*]Corresponding Author: rahees.mohdkhan786@gmail.com

Abstract. *These days, there are a lot of similar applications and concepts being used, which increases the threat of cyberattacks. Even slightly different attacks and threats can cause major issues for the network as a whole, which is why security system concepts are crucial. The current analysis aids in the discussion of IoT network security management, breaking it down into five sections. We usually start by illuminating the history and premise of the Internet of Things. The requirements for IoT security are then discussed. The anticipated design may be expected to return once safety management has been clarified in the following section. The security of the Network Cryptography system then leads us to implement web protocol security. A detailed explanation was also given on how this projected design might be used in the future with appropriate safety management for the Internet of Things network.*

Keywords: *IoT, security and management, threats and attacks, design and layers, network security, science security, Cryptography.*

Introduction

The Internet of Things safety management system may be supported by the architecture of the network infrastructure (IoT-SMS). The IoT network structure has five distinct security concerns, all of which are taken into account before a system of security management is set up. Protection concerns like these compute that high-quality square sensors are easy to compromise, security monitoring can support low-power systems, privacy concerns with partial layer devices, risks associated with completely separate layers, and issues with system complexity and compatibility [1]-[5]. According to these specifications, our goal is to create an IoT eco-system protection monitoring framework that complies with IoT standards and guards against any potential threats. Stated differently, the network security management should be designed as a bedded framework on equal lines because the Internet of Things (IoT) network environment is meant to be a four-layer device architecture. [6] [7] For the IoT ecosystem, we would rather propose a four-layer protection management scheme that incorporates this idea, similar to the one used for IPsec's functional nature. The planned IoT protection management framework consists of four functional levels (IoT-SMS). The following were the concepts that were put into practise to create the four square measurement layers: a layer of

practicality is formed whenever a special, unique, and distinct kind of security functions are needed at a different level. Every layer carries out specific safety procedures. For the current uniform protocols, each layer's practicality is carefully chosen. The layer boundaries are chosen in order to reduce the information flow through the device interfaces. The number of layers aligns with the IoT framework's layers in a way that eliminates the need for different protection tasks to be carried out inside the same layer.

IoT Layers Reference Model

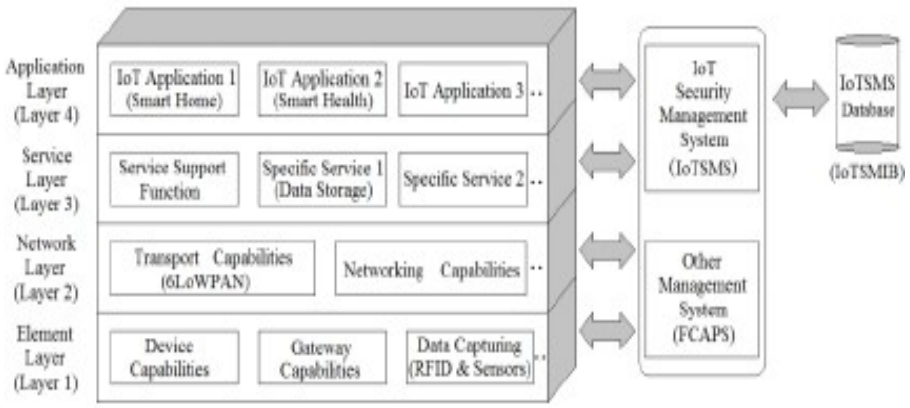

Fig. 1. The IoT Layered Reference Model

IoT Layered Architecture

Each layer's components, guiding principles for coordination, and procedures are described in detail below. The stratified design has the following advantages: supplying standard management for the Internet of Things. We'll implement multiple security protocols and security services frameworks at any layer to increase the overall security of the IoT network infrastructure [8]. Because the stratified system is extensible, higher layer facilities are provided to the lower area unit. Permitting the most recent technological advancements to be integrated into a widely used IoT network infrastructure for every hardware and software system makes the layered structure easy to manage in a reasonably sensible deployment still in part [9].

Element Layer

The lowest IoT layer is the component layer. This layer of the system is made up of various nodes and sensor types, including barcode labels, RFID, actuators, and smart detection systems. Due to their design, these square measurement sensors are unable to assess artefacts as they transfer the gathered data to the subsequent layer. Information is gathered by modules and sent to the network layer [10].

Network Layer

The network layer is in charge of sending the information gleaned from the component layer to the higher 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. Measureability is required by an IoT [11].

Service Layer

It is made up of functions that process the information obtained and offer storage connections for the information obtained from the component layer. The Internet of Things (IoT) layer offers communication channels between weather stations and acts as an interface between the different IoT devices. The service layer sits atop the network layer and provides a property between sensors. Additionally, it provides services to guarantee effective, purposeful communication between devices and apps. We'll discuss the "Open Remote" as an associate degree example of a service layer implementation for the associate degree RFID device, similar to the middleware response for commercial and residential buildings and automation [12].

Application Layer

The platform layer is made up of several IoT smart apps that have facilitated customer needs. The application layer makes use of numerous protocols, including XMPP, MQTT, AMQP, and CoAP [13].

Data Flow between Layers

The four stages of the Internet of Things data flow are knowledge transfer, knowledge preservation, knowledge review, and information assortment. For the information assortment and storage to carry out the purported five familiar network management (FCAPS) functions, fault, setup, accounting, efficiency, and protection management functions are required [14].

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, andprofit 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 orcondemn 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 ofend 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].

IoT Security Management System

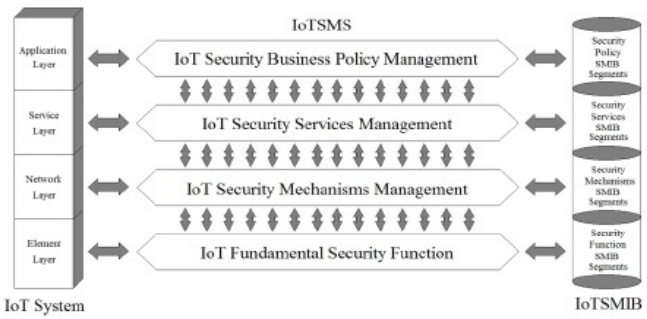

Fig. 2. Security Management System for IoT

The design of the IoT network structure, which consists of four layers, has been demonstrated. There are three components to the architecture for security management. The four levels of defence business plan management, IoT security services management, elementary IoT security efficiency, and IoT security system management comprise the middle half of the IoTSMS. Such as mutual, regular arithmetic output, and pseudorandom generators, each layer has its own practical application in protection management to guarantee information confidentiality, reliability, and usability. The SMIB uses the IoT protection management database and the X.509 version three recommendation authentication on the diagram's right side (SMIB).

Functional Layers of Security Management for IoT

The square, as previously mentioned, evaluates four IoT protection control tiers. These are the operational layer of basic IoT security, the management layer of IoT security mechanisms, the management layer of IoT military intelligence, and the management layer of IoT corporate strategy. To safeguard the IoT security management framework, each layer is involved in its own set of tasks [8].

Requirements of IoT Security Business Policy Management

The business customer's needs, such as interference and preventing risks from attacks for very different purposes, maintaining the privacy of all successful computers, safeguarding the IoT infrastructure from attacks, and averting system failure, are the focus of the security business decision management layer.

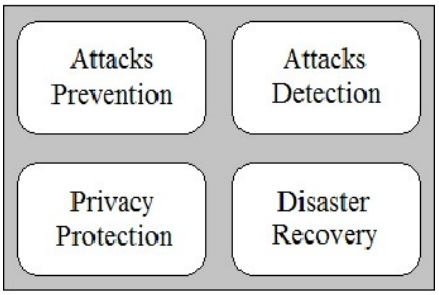

Fig. 4. IoT Security Business Policy Management Requirements

IoT Security Services Function

The useful layer component of IoT defence services includes the most crucial security services, like peer agency and data root authentication in addition to authentication services. Perhaps the most widely used aspect of IoT security is confidentiality, including selective filed confidentiality. The information within an IoT environment is constantly changing. In this context, service of dignity implies that improvements can only be made through authorised mechanisms. In addition to relationship integrity, connectionless integrity, and selective filed integrity, non-repudiation services like origin and destination non-repudiation, and even access management programmes, are crucial for the security of IoT systems.

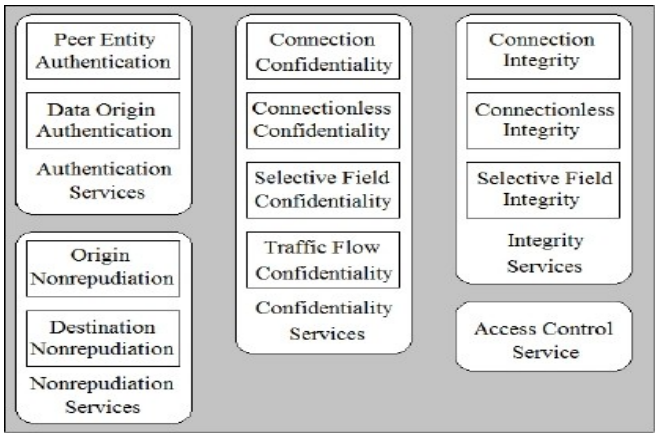

Fig. 5. IoT Security Services Functionality Layer

IoT Security Mechanism Function

The protocols, algorithms, and schemes needed to enable the security services outlined in the layer of security services are present in security structures. The security mechanisms, or ubiquitous mechanisms, are provided by the layer of the IoT protection framework's practicality. Decryption, digital signatures, access control, information integrity, identity sharing, traffic objects, routing management, and security protocols for notarization are examples of precise protection measures. Indeed, among the widely used security mechanisms were host intrusion detection systems, practicality, security marks, identification, security audit routes, networks, and security recovery mechanisms.

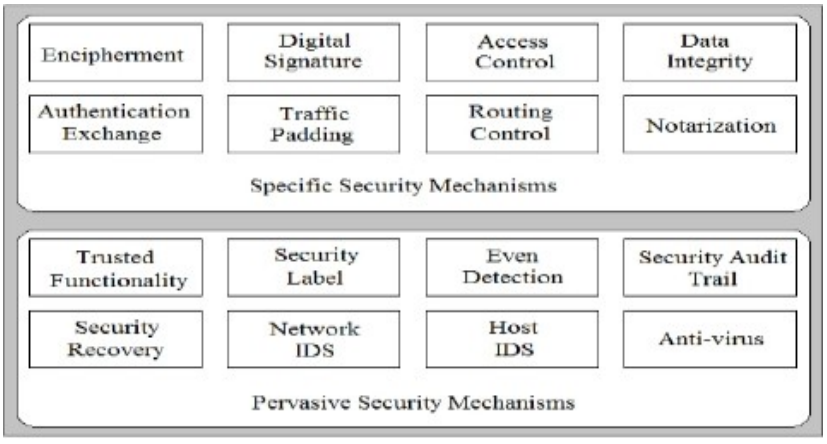

Fig. 6. IoT Functionality Mechanisms Layer

IP Security Implementation

A secure hashing function in tunnel mode is used to modify the IP packet header section while cryptographic checksum techniques are used to compute the packet data and headers to be sent. In order to authenticate the recipient with the data from the regular package, it appends a new header with the hash value. It appears to establish a unique tunnel on a public network that is exclusive to a certain group of users. An example of an IP Security usage diagram for constructing secure communications over public networks is shown in the figure below. 192.168.10.1 and 192.168.20.1

are the local IP addresses used by private networks #1 and #2. Both gateways are easily accessible from any computer with an internet connection because they both use public IP. To connect from internal network #1 to #2, there are a few steps involved. It is necessary to encapsulate each packet sent to IP 192.168.20.1 into another packet in order for the public IP X.X.X.X to appear in the IP header. After that, it will be routed via a gateway to public IP Y.Y.Y.Y, where the IP header will indicate that the packet originated from IP X.X.X.X. We refer to this procedure as encapsulation. For the gateway to reach IP 192.168.20.1, it needs to know the path. The packet needs to be redirected to IP 192.168.20.1. It produces a unique tunnel that connects the two networks. After the connection is made, both networks are able to ping each other and communicate. To get the actual packet, the packets must be encapsulated when they arrive at IP Y.Y.Y.Y and sent to IP address 192.168.20.1. [11].

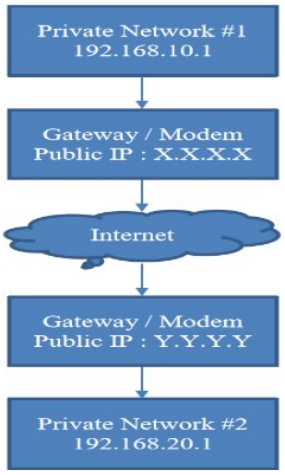

Fig. 7. IP Security Implementation [11]

Fundamental IoT Security Function

Since it could provide better security to multiple applications at once, a basic SMS IoT feature was used in an independent comprehensive security server. So, many generic cryptography and arithmetic modules were incorporated into a very low-cost practicality layer. Basic security features such as message digests, unidirectional hashes, and secure hash algorithms are provided by an IoT elementary security. The RSA, Diffiedramatist, and elliptic curve algorithms work together in the layer to provide key exchange security. The enclosed information includes timestamping, certificates, authentication codes, message authentication, elliptic curve algorithms, and the digital signature and X.509 certificate normals. The layer included every cryptologic function required for the Internet of Things SMS to operate.

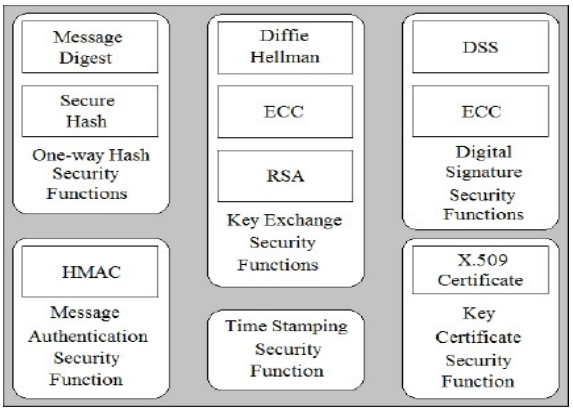

Fig. 8. Fundamental Security Functionality Layer

IoT Security Management Information Base

The IoT SMIB is a crucial component of the Internet of Things. This information can be used to create applications for all IoT security services that are applied in highly computational environments or contact settings. Critical sensor IDs, user accounts, security logs, and access management lists are all abstracted into the IoT Protection Management Info Base [12].

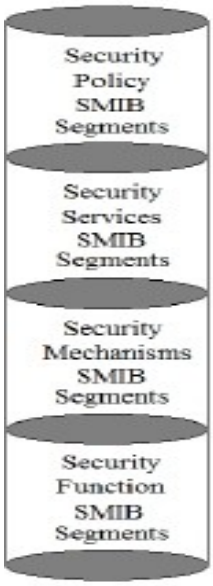

Fig. 9. The IoT SMIB Segment

PKI for the IoT Security

The Engineering Task Force (IETF) created the General Public Key Infrastructure (PKI) to create a paradigm of confidence for many. [14] Even though the security of the Internet of Things is important, PKI's primary output is the provision of X.509 keys, key storage, and upgrading, as well as the delivery of services to specific protocols and access control. By using malicious coding and authentication in communications, PKI provides a straightforward method for data protection. Because it has PKI in place, the IoT device is resistant to destructive and brute-force attacks. PKI

provides access to the protocol and programme setup that is still user-friendly while ensuring the integrity of the data collected by the sensors and lovely devices. Additionally, PKI upholds the confidentiality of the portion layer within the Internet of Things. A variety of mathematically connected public-private keys are provided by PKI. Only the opposite associated key will be able to decode the information if it is used to encrypt one key. In the case of the component layer inside the IoT framework, the information collected by the sensors and successful devices is protected using a public key; as a result, the non-public key to decipher is misused.

Advantages of the Modular Security Management System for IoT

The architecture for IoT protection management provides a standard framework with multiple security resources and multiple security monitoring frameworks. Consequently, protection standards for network providers, vendors, and product manufacturers were introduced. Several Security Service management modules can call independent security framework modules to evaluate the best security requirements and IoT network framework management by introducing the affordable elementary protection operation. With the help of customer security requirements, the IoT-SMS standard protection management system integrates affordable monitoring techniques and procedures within the IoT network system. As new techniques and technologies emerge, the anticipated IoT-SMS would also support additional protection. It provides a consistent framework for protection in the context of the Nursing IoT device Associate.

An IoT Security Management Scenario

Examine a reasonable scenario for managing home security. The home's owner wishes for guests to respect the level of comfort in his residence. [13] However, because the property owner is in that specific location, he or she must use a mobile device to monitor the lighting, weather, and level of moisture in the home.

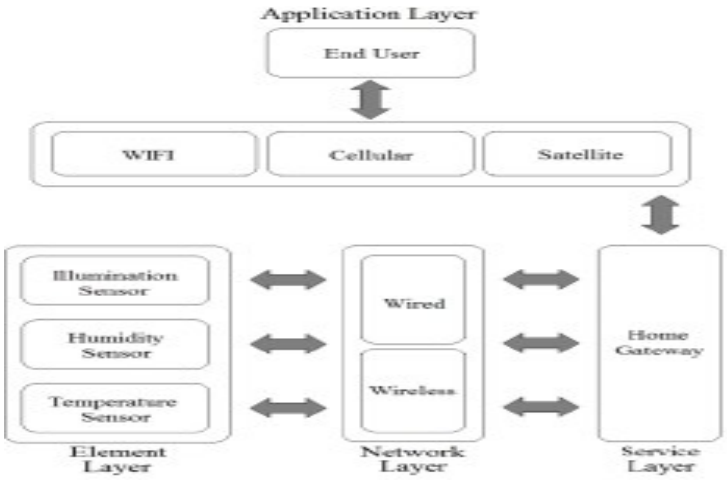

Fig. 10. Concept of the Smart Home Scenario

Protocols Used in the IoT SMS Scenario

In order to meet the requirements of low-power and low-speed sensitive devices inside the component

layer, we instead choose to use the IEEE 802.15.4 wireless networking protocol, which includes the necessary protection services of anonymity, authentication, and honesty. At the network layer, we prefer to use the 6LoPWAN protocol, which introduces the low-power and lossy network routing process. In order to offer secrecy and reputation protection services, the routing system integrates AES for a raincoat with 128-bit keys and supports RSA for digital signatures with SHA-256. In order to minimise the specifications for information estimation and resource-constrained systems and low-power devices, we prefer to use the CoAP protocol, which operates over UDP in the application layer. In order to provide the previously mentioned protection services, the CoAP protocol uses the AES cryptological formula and provides a contact paradigm of "request and response" between the endpoints.

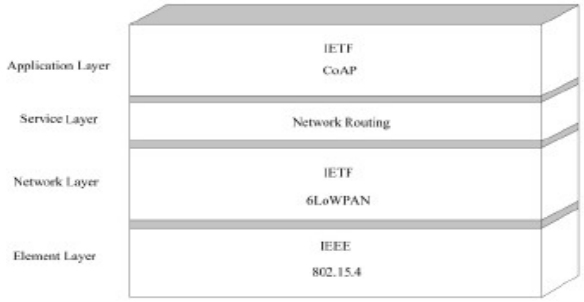

Fig. 11. Protocols Used in the Smart Home

Data flow by the Smart Home scenario

Various sensors record environmental data, such as temperature, lightweight pressure, and vapour concentration. After that, a unidirectional hash that is called within the component layer by an authentic service management module processes the data to create a digital signature message. The IEEE 802.15.4 protocol is implemented by the symmetric-key cryptosystem AES. The comprehension that originates from the component layer is encrypted abuse that the standard concealed writing performs, called upon within the network layer by the identity integrity service management module. The routing system of low-power and lossy networks, which uses AES with 128-bit keys to provide secrecy and authentication services for integrity, is incorporated into the 6LoWPAN protocol [14] [15]. The accessibility service management module even calls the operating module of the "Network Intrusion Detection System" (NIDS) to prevent the DoS attack during the transmission through the internet, local area network, or cellular network after the service layer obtained the encrypted information. The primary certification authority module is triggered by the authentic framework of service management within the application layer in order to verify the customer's identity by looking through their user profile. The private key that the PKI module uses to victimise messages is then decrypted by the user. A coordination model for "request and answer" between the endpoints is provided by the CoAP protocol. Under the protection of economic security, the user can remotely monitor the temperature, humidity, and lighting within the home using the API appliance on a high-quality phone.Various sensors record environmental data, such as temperature, lightweight pressure, and vapour concentration. After that, a unidirectional hash that is called within the component layer by an authentic service management module processes the data to create a digital signature message. The IEEE 802.15.4 protocol is implemented by the symmetric-key cryptosystem AES. The

comprehension that originates from the component layer is encrypted abuse that the standard concealed writing performs, called upon within the network layer by the identity integrity service management module. The routing system of low-power and lossy networks, which uses AES with 128-bit keys to provide secrecy and authentication services for integrity, is incorporated into the 6LoWPAN protocol [14] [15]. The accessibility service management module even calls the operating module of the "Network Intrusion Detection System" (NIDS) to prevent the DoS attack during the transmission through the internet, local area network, or cellular network after the service layer obtained the encrypted information. The primary certification authority module is triggered by the authentic framework of service management within the application layer in order to verify the customer's identity by looking through their user profile. The private key that the PKI module uses to victimise messages is then decrypted by the user. A coordination model for "request and answer" between the endpoints is provided by the CoAP protocol. Under the protection of economic security, the user can remotely monitor the temperature, humidity, and lighting within the home using the API appliance on a high-quality phone.

Conclusion

A significant part of this investigation is the delivery of a comprehensive security useful design that is also extremely straightforward security management strategies for an Internet of Things network. This is an important component of the investigation. The reason for this is to ensure that all of the requirements that the users have for the network providers are met. The science security protocol is situated within the network layer, which extends from the lowest layers to the highest layers of the Internet of Things network. It is possible for the protection management system of the web of things to safeguard (the information, the data, and the information) from the lowest layers all the way up to the highest layers. The earliest layers of the Internet of Things network demanded privacy and were also firmly protected by a variety of services, mechanisms, and policies within the network.

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 Com- munication 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.