International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-6, August 2021

Data Protection Mechanisms in IoT: A Vital Challenge

M. G. Padmashree, J. S. Arunalatha, K. R. Venugopal

Abstract*: The Internet of Things (IoT) associated with life is a budding real-time environment paradigm. Smart Users can control and analyze Things through Smart gadgets connected through the network. As gazillions of devices are connected and communicated via a complex, distributed network, the number of potential threats and attacks has grown drastically against protection and privacy. Security must be provided continuously for IoT service. Exploring the issues to be improved in IoT setup includes Information Secrecy, Access Control, Authentication, Integrity, Privacy, and Trust. The paper summarizes the issues with IoT device security and the efficiency of the existing security solutions. This paper analyses the schemes to guard IoT communications and the methods adopted by the researchers while providing security of data in IoT.

***Keywords*: Access Restriction, Authentication, Identity, Key Management, Lightweight Cryptography, Security**

I. INTRODUCTION

Network technology has evolved from connecting computers using the Internet to connect SmartPhones and various gadgets with the same communication ability. A novel paradigm Internet of Things connects virtually associated autonomous, heterogeneous smart physical devices connected to the Internet that responds intelligently. There is no standard definition for IoT, and still emerging. A system is considered as the Internet of Things if it has the following features: Interconnected Things, Devices to Internet Connectivity, Distinctive Identification of Smart-devices, Ubiquitousness, Detection/Actuation Ability, Embedded Intelligence, Potential to Knowledge Incorporation, Self configurability, Programmability. A billions of devices connected and communicated increases the viable risks of attacks drastically contrary to security and privacy [1].

Oualha *et al.*, [2] stated that a Data Access Control solution manages enormous IoT devices using Ciphertext-Policy Attribute-Based Encryption (CPABE). Source encrypts data to enforce secure access. Data User, authorize with intended attributes, decrypts data cryptographically. However, CPABE requires more energy, and most of the IoT devices, *viz.*, sensors, actuators have resource limitations: CPU, memory, battery, *etc.*, Choi *et al.*, [3] proposed the use of the Data Encryption Standard scheme that reduces the payload of an increase in Ciphertext size with attributes. Mosenia *et al.*, [1] summarized IoT security concerns of Nodes, Communication, Computing and its countermeasures against them *viz.*, Trojan Activation methods, Blocking, Role-based Authorization, *etc.*, Simple protection processes with limited resource usage enhance security for IoT applications [4].

There is a need to consider the complexity and energy limitations in security designs. No universally stated metric decisively portrays the computational intricacy of a chosen ciphering and deciphering technique.

Security threats are challenging for IoT due to Things with insufficient resources, the physical availability of Sensors, Actuators, the receptiveness of frameworks, and wireless communication. The security problem further exacerbates as the temporary and stable arbitrary malfunctions are misused by intruders [1]. The two lightweight communication protocols used for IoT applications are COnstrained Application Protocol and Message Queue Telemetry Transport, which lack Peer-to-Peer security between IoT brokers and IoT devices [3]. IoT applications must be able to provide suitable service on security attacks successfully. The system must be proactive and reactive to novel attacks.

The main objective of the paper is to brief the state-of-the-art of security scenarios in IoT. Security must be all over the IoT life cycle from the early proposal to the maintenance phase [9]. The issues to tackle in IoT setup *viz.*, the Access Control, Authentication, Key management Attacks, and Countermeasure techniques are analyzed comparing various approaches.

The paper is structured as follows: Section II presents the different Related Security Frameworks and architecture. Section III describes the Authentication methods used to secure the IoT, Section IV presents existing Key Management techniques, and Section V explains the Access Control mechanisms. Section VI discusses Security Attacks and Counter Measures; Section VII provides the Result Analysis of the Security solutions and challenges; Section VIII concludes.

II. RELATED SECURITY FRAMEWORKS

There is no generally accepted framework for the implementation of secure Internet of Things. A reference architecture shown in Fig. 1 indicates the need for Authentication, Access Control, Data Encryption, and key management for the resilience of security attacks.

Manuscript received on July 27, 2021.
Revised Manuscript received on August 17, 2021.
Manuscript published on August 30, 2021.
* Correspondence Author
M G Padmashree*, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru, India, Email: padmashree.mg@gmail.com
J S Arunalatha, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bengaluru, India, Email: Email: aruna_veeresh@yahoo.com
K R Venugopal, Vice-Chancellor, Bangalore University, Bengaluru, India, Email: venugopalkr@gmail.com

Fig. 1. Security Modular Architecture for IoT

Aman *et al.,* [5] compared Game-based, Requirements-driven, Event-Driven, Ontology-based, and Context-Adaptive Security Frameworks to determine the security and architectural capabilities. The evaluation framework assesses the feasibility of versatile security models in an IoT environment. For several models, all the risk management components were not unhandled to adapt completely and did not provide a threat assessment detail for risk management. Chamberlain *et al.,* [6] implemented the EZConnect security infrastructure with multi-level security, setup, and operation. The serial number of the Controller and Authentication Code is required to use the Application remotely. The Equipment Manager entirely controls remote access. A Brute-Force attack is harder on Access Code with a stronger Character Set. Exclusive methods confines interoperability. Comprehensive Security and Privacy-Preserving Architecture [7] guarantees strong security, privacy preservation, and resilience in the presence of strong adversaries without considering the supporting User incentive mechanisms. Ye *et al.,* [8] presented a Three-Way handshake that certifies the exactness of the keys exchanged and prevented invaders from copying new data, leading to inconsistency during the exchange of data in a session and enhances the protection of keys during key exchange. It is hard to get complete data without attacking Receiving Node as the data travels through multi-path.

Tiloca *et al.,* [9] presented a Security Architecture that addressed vulnerability to Denial-of-Service, scalability on the Server-Side, and the issues of DTLS handshake to reduce the effect of Denial-of-Service (DoS). A shorter duration than a DTLS protocol is required to contract with improved DTLS Server protection. The Server accumulates the single Pre-Shared Symmetric Key. This method does not necessitate alterations in DTLS standard or extra DTLS Client-Server interaction deployable in the TLS protocol. The existing Handshake does not validate the genuineness of the DTLS Client. The effect of DoS reduces on using Reactive strategies. Alpár *et al.,* [10] designed a framework to integrate Attribute-based Authentication in the IoT Architecture to significantly reduce the privacy compromise caused by the transactions linked to the same identifier are traceable as Authentication is the proof of identity information and ultimately make the users identifiable.

Han *et al.,* [11] proposed a Security Protocol that used Hash Function, Passwords, and Time-Stamp to verify and validate the Sender and the Receiver before the communication. Session-Key and Public-Key virtually prevent the attacker from meddling the transmission and execute hacking attacks. The complexity of the protocol can be reduced further by incorporating simple formulas. Attack-resistant characteristics can provide efficient and robust Authentication. Johnson *et al.,* [12] proposed a flexible strategy for Field Programmable Gate Arrays, appropriate for IoT. Two Dynamic Partial Reconfiguration architectures are secured and appropriate for IoT applications with less overhead. It is resilient to Hardware Trojan Insertion attacks. Moosavi *et al.,* [13] proposed Three-Tier System Architecture ensuring security using the Certificate and the Session Renewal. Ubiquitous mobility achieves without reconfiguring the device layer. It consumes almost half of RAM and one-third of ROM resources as consumed by certificate-based DTLS and the same as that in Symmetric-Key-based DTLS. The drop-out latency caused by portability is low without inducing any overhead and ensures peer-to-peer security.

Hernández-Ramos *et al.,* [14] proposed a Framework with a group of suitable Authentication and Authorization mechanisms integrated and extended to tackle different security issues of Smart constrained devices. It is a decentralized approach to provide the advantages of a distributed perception *viz.,* adaptability, scalability. The framework ignores the Network Admission Control security components of the structure. Gope *et al.,* [15] proposed the Authentication scheme with an enrolment stage to acquire identification by a Sensor Node, mobility of the Nodes between the Clusters of the same network retaining its identity, and the mobility of Nodes between the networks. Performance is better than RSA and Elliptic Curve Cryptography (ECC) Authentication schemes in security and computation overhead, appropriate for the nodes with limited resources in distributed IoT systems.

Polyzos *et al.,* [16] described Three security solutions: Access Control Enforcement, Secure Information Proxies, and Reliability. The Things rely on delegating different services to others due to their restricted computation and storage capacity. Applying ICN in Client devices and Access Networks brings significant performance improvement, Access Network planning, deployment, application adaptability, and security. Zhang *et al.,* [17] focused on protecting the Internet of Things traffic to implement a Peer-to-Peer Security Protocol to meet the complex requirements from applications, diversified devices, and suitable communication environment by avoiding extra Handshake in future sessions and dynamic security level adjustment. The security communication is four times faster than TLS, and Users preserve confidentiality in IoT. Sicari *et al.,* [18]'s novel IoT Architecture, fulfilling the security features of Data Transmission, supports protection, confidentiality, and integrity assurance.

Retrieval Number: 100.1/ijeat.F30200810621
DOI:10.35940/ijeat.F3020.0810621
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

A. Lightweight Cryptographic algorithms

Data encryption provides data secrecy. Choi *et al.*, [3] proposed a Framework that converts User data with Advanced Encryption Standard and its Keys exchange after applying CPABE. IoT Broker cannot recover the data unless all attributes of IoT device with a unique identification. IoT Certificate Authority manages and issues an Attribute Certificate using ABE. This scheme protects from Eavesdropping and a malicious IoT Broker. It introduces a response time delay compared with models without Encryption. Liu *et al.*, [19] implemented ECC Group operations, a High-Speed version, which achieves less computation cost for Cryptographic schemes. The security and effectiveness of low-level Field and Group Arithmetic operations depend on the proper selection of Curve models and domain parameters. The Twisted-Edwards-Montgomery models of Elliptic Curves increase the performance, reduce the storage, and energy consumption in the IoT environment.

He *et al.*, [20] analyzed the security of Elliptic Curve Cryptography-based RFID Authentication schemes and implemented for comparing the communication and computation costs of RSA. Most of the ECC-based Authentication schemes have acceptable attainment but are undefendable to all security breaches. Chakraborty *et al.*, [21] provided a uniform platform for Advanced Encryption Standards and the Intel AES-NI instructions to achieve authenticated Encryption with associated data. The existing frameworks are not standard or generally accepted frameworks. The comparisons of five different existing security frameworks are shown in Table I.

The security relies on Authentication, Data Secrecy, and Access Control techniques. Cryptic functions provide Data Secrecy, but key management is the issue.

III. AUTHENTICATION

An architectural model for the authentication process is shown in Fig. 2. The Keyed Hash scheme without a Certificate Authority (CA) [22] provides complicated Authentication with an efficient Security level, Power consumption, and Code size. It solves the security issues when a heavy load is allotting to the role of the left CA. This scheme cannot apply in evolving environments, *viz.*, BLE or Zigbee. Aman *et al.*, [23] proposed Physical Unclonable Functions (PUFs) Mutual Authentication Protocol that provides security from Physical, Side-Channel, and Cloning attacks. PUFs perform with low computation, communication overhead, and storage requirements. PUFs realize efficient and strong security protocols, *viz.*, RSA for IoT devices. Tian *et al.*, [24] designed and deployed a hardware and software, Security and Privacy Protection Platform, using privacy queries and privacy authentication, the basic security measures, privacy-protection, intrusion prevention, and malicious code precaution technology of wireless network. The basic security measures, intrusion prevention and, malicious precaution implementations secure the system.

Wu *et al.*, [25] suggested an Authentication Scheme employing the Random Oracle Model. The User, the device, and the Broker are mutually authenticating before they communicate. Lu *et al.*, [26] propose Safeguard, an efficient and transparent re-Authentication Scheme using the Behavioral Biometrics provided by Sliding Dynamics and the pressure intensity on Touchscreens with Support-Vector Machine Learning algorithms. The User is verified by Safeguard with almost no False Acceptance and Rejection Rate within 300ms, having less than 20 slides. This system can effectively resist Adversary imitation. The systems storage and computation overhead are feasible. Giri *et al.*, [27] propound a Mutual Authentication scheme that efficiently encrypts files and restricts data attainment without authorization, thus accrediting protected and functional USB storage. Users can store their encrypted data after the authorization process. The data in encrypted form can be accessed in the active session and over multiple sessions, with a reduction in communicational overhead. The usage of the device increases across contrast sessions. It has relatively less computational and communicational overhead.

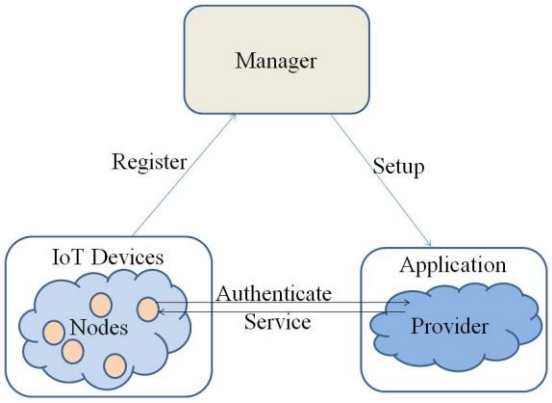

Fig. 2.Architecture model for Authentication

Gope *et al.*, [28] proposed a Pragmatic Unknown User Authentication scheme that guarantees various security features *viz.*, User Obscurity, Underivability, Rearward Secrecy, and excellent Forward Secrecy. It provides security from attacks, reduced processing, and execution cost compared to the existing schemes. It is suitable where the valid person is authorized to obtain the sensor information from nodes in a resource-restricted device community. Wallrabenstein, [29] propound the Elliptic Curve Cryptographic Protocols based on Physical Unclonable Functions for resource-constrained modules. In PUF-based protocols, private key exposure minimizes; tamper resistance is cost-effective. Gasti *et al.*, [30] submitted a confidentiality maintaining Authentication Scheme, which ensures resilience from an attack without using Two-Party Protocol, Cut-and-Choose. Authenticating Users is faster. However, it is appropriate for non-stop Smartphone User Authentication with a Window of one minute. It consumes minimal energy in the circuit for the offline charging Smartphone. Thus provides reasonable power usage and processing speed.

Table- I: Security Framework Summary

Article	Method	Advantage	Disadvantage
Chamberlain *et al.*, [6]	multiple layers of security measures	Users of the remote Application need only the controller serial number and authentication code	vulnerable to brute force attack, proprietary mechanisms limits interoperability
Choi *et al.*, [3]	CPABE and AES encryption with Certificate Authority	offer protection from intruders and a compromised gateway	introduce a response time delay
Gisdakis *et al.*, [7]	Pseudonymous Certification and Group Keys	withstanding the attacks from adversaries	No supporting User incentive mechanism
He *et al.*, [19]	ECC-based authentication schemes	Satisfactory performance	Exposed to malicious attack.
Kothmayr *et al.*, [30]	Two-way Authentication with EC-DH key exchange and ECDSA	Provides message integrity, confidentiality, authenticity and avoids MITM	network overhead introduced

Peng *et al.*, [31] proposed a User Authentication System to scrutinize gesticulated and articulated inputs. The Threshold Random Walking technique chooses from multiple User Events only if it is confident. GlassGuard identifies the possessor and fraud using a few gesticulated and articulated instructions of User interactions.

Amin *et al.*, [32] contributed an efficient architecture and designed a defended 3-factor User Authentication Technique. to protect from active and idle intrusions. The protocol consumes reasonable power consumption of IoT devices, Communication, and Memory Overhead. Relevant functionalities *viz.*, Log-in, Key Revocation, Mutual Authentication, Session Key protection, and new Node are achieved, But vulnerable to Playback and DoS attacks [33]. Authenticated Key Exchange scheme [33] defeats the security problems of Amin *et al.*'s [32] method and Farash *et al.*'s [34] method. It has 14 Hash less than Amin *et al.*'s protocol, 15 Hash less than Farash *et al.*'s [34] protocol, and two more Random Generations with acceptable efficiency. It is resistant against Replay, DoS, Un-traceability attack, User, Sensor Node, and Gateway Impersonation.

Lightweight Authentication Scheme [35] allows verification of both devices and distant Clients for secure communication in a resource-constrained environment. This scheme maintains integrity in Key Distribution using a nonce, Pseudonymity, XOR operations, and Secret Hash Message Authentication. The Hashed Message Authentication Code obtain by applying repetitive Hash Function, *viz.*, MD5, or SHA-1, once a session key is established to provide Authentication with much lesser power usage. It has less memory consumption and execution time. Ren *et al.*, [36] presented an Authentication System to secure by verifying Voice and revise it by a Dynamic Threshold (DT) method. Revised DT method trim down the False Rejection Rate with the specified False Acceptance Rate.

Chang *et al.*, [37] proposed an Authentication scheme with two modes to withstand Identity attacks providing Perfect Forward Secrecy. The first mode does not require the Broker to possess information on keys used. It involves Pre-Launching, Enrolment, Verification, Validation phase, and Secret Revocation process. It does not offer optimal Forward Secrecy, and it is lightweight. The other mode guarantees faultless Forward Secrecy and shares the Pre-Launching, Enrolment, and Secret Key Revocation stage of the first. The two operational modes are required in an Authentication Protocol to provide a higher level of security. These are deployed on a device with minimum memory expense depending on the Application's security needs. Ceccarelli *et al.*, [38] defined a protocol by exploiting Biometrics in Session Management for Uninterrupted Authentication to improve Session and provide protection. The Certificate is recognized utilizing Time Stamp and Nonce [39] with a Timeout depending on the reliability of the User behavior to defend the Replay attack. The system exchanges raw data. The Client device temporarily uses sensors and transmits data on Internet, introducing un-quantified power usage. Battery consumption and User profile are the limitations. Gehrmann *et al.*, [40] presented a Short Message Authentication Check (SMACK) sustainable with a reasonable memory, power, and computational overhead. It avoids device interaction in identifying void messages requiring few computations. The proactive DoS attack measures and renewing long-term key material are ignored.

Farash *et al.*, [34] improved Authentication and Key Agreement (AKA) protocol for a diverse environment that incorporates four-step between User, node, and gateway authentication; every registrant directly interacts with an IoT device bypassing the IoT Broker. The Hash and XoR computations are lightweight and require less storage to accumulate large data at a high instance. The existing Authentication schemes do not provide sufficient security for the IoT. The comparisons of different existing Authentication schemes are shown in Table II.

IV. KEY MANAGEMENT

An architecture model for the Key Management process in the IoT is as shown in Fig. 3. Iqbal *et al.*, [41] introduced a Key Establishment scheme that is secure through strong Encryption and Authentication. The resource-constrained nodes benefit from the same security functionalities common in unconstrained domains without executing computationally intensive operations. The cooperation with the neighboring trusted nodes or devices offloads massive Cryptographic operations of constrained nodes. Castiglione *et al.*, [42] proposed a Hierarchical Key Assignment that supports Dynamically Updating Access Structure. Class/Edge Insertions/Deletions to inter Class access propagation, replacing the keys and User revocations use Graph-based Two-level Symmetric Encryption. The security outstands on Key indistinguishability, Key Generation and Derivation. User accumulates at most one private key.

Table- II: Authentication Schemes Summary

Article	Method	Advantage	Disadvantage
Jang *et al.*, [22]	Hash scheme with keys and without a Certificate Issuer	Power consumption and Code size are less; handle the overloaded role of the left CA.	Cannot apply in continuously evolving diverse environments. The Key agreement for the security platform is not considered.
Khemissa *et al.*, [35]	used nonces, masked identity, XoR operations, and Secret Hash message authentication	energy-efficient; protection from many attacks; reasonable communicational and computational cost; less memory consumption.	Not tested in a real deployment.
Amin *et al.*, [32]	three-factor identity Authentication	Secure from dynamic and static attacks; reasonable power consumption by the sensor node, processing, storage cost, and execution time; Provides proper mutual Authentication and session key safety.	Vulnerable to Replay attack and DoS attack.
Farash *et al.*, [34]	improved validation and key management protocol incorporating four-step sensor node first authentication model with Hash and XoR computations	Protection from typical attacks.	Insecure against forgery attack; cannot preserve User anonymity property.

Raza *et al.*, [43] proposed a Key Agreement scheme, Scalable Security with Symmetric Keys (S3K), enable devices to use DTLS with derived keys and public keys established and authorized. S3K is scalable to apply in resource-constrained devices. Pre-provisioning multiple Pre-shared Symmetric Keys (PSKs) and confirmation of Shared ASymmetric Keys in a separate stream are not required. The Key Generation process does not affect the time taken for a DTLS handshake. The DoS attack can inject.

Identity Ring, Secret key of Sender, and Shared Secret of the Receiver achieve confidentiality, non-repudiation, unforgeability, and anonymity [44]. Key Administration conspire [45] between the device and an associated Smart node, accomplishing Forward and Reverse Key Detachments and protection from Jamming between the Relay and the Smart node. The processing cost of the device is directly proportional to the magnitude of devices with the same quantity of Relay nodes. Hence reduces the computational complexity, the communication overhead, and resistance to the collusion attack. The Relay node requires extra storage for the re-encryption key.

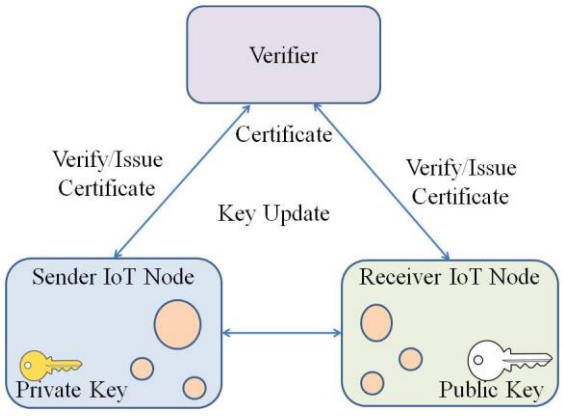

Fig. 3. Key Management in Internet of Things

Iqbal *et al.*, [46] designed an AKA protocol resistive against MITM, Sybil Attacks, and Eavesdropping. The Secret Keys passed in multiple chunks. The communication overhead due to Trusted Sensors Identity exchange not considered. Buchmann *et al.*, [47] replaced the Gaussian Noise Distribution in the Learning with Errors over Ring-based Encryption. The Polynomial Multiplication algorithm is simple, and the mapping of polynomial coefficients in assembly implementation did not reduce the storage requirements. Double coefficients store in a four-octet than an individual coefficient in a single byte data word increase the Key storage requisite.This scheme consumes more execution time compared to Lattice-based Cryptography since high-level optimization. It outperforms with fewer storage requirements than a code-based scheme. RSA-1024 Encryption outperforms in terms of memory consumption but with reduced execution time. The rapid implementation requires more storage space, and the memory-efficient takes more execution time. Barki *et al.*, [48] compared the scalability, robustness, appropriateness considering the IoT restrictions. Group Key Management for expandable safe group communications is unaddressed.

Qiu *et al.*, [49] used Hybrid Cryptography to secure information exchanges where the Remote Server with a Session Key between the devices. This scheme is safe and can avoid attacks: Replay, MITM, Impersonation, and Sybil attacks. Ning *et al.*, [50] designed a dual strategy to provide lower to upper security for singular and universal layered IoT architecture. The Aggregated-Proofs attain secret data transmission on various nodes. The structure-preserving Chebyshev Chaotic Maps with specified route details achieve validation. Admission is controlled hierarchically by assigning various authoritative entries. Every session is secure by using dynamic Hash Keys. Jr *et al.*, [51] analyzed the agreement without CA and showed that the Strengthened-Menezes- Qu- Vanstone and Implicit Certificates increase the efficiency. The Key Distribution cost is less compared to the schemes that use Certificates based on traditional PKI. AKA schemes with A Key Generator (KG) produces Shared Secret using Consumer ID attested by KG, and the Consumer produces Secret Code based on individual Secret [52].

Li *et al.*, [53] implemented a GRoup-based Authentication and Key Agreement protocol (GR-AKA) with the Diffie-Hellman Key Exchange to achieve Congestion-Avoidance Authentication and Dynamic Access-Policy Updating and Session Key Establishment.

Communicating devices authenticate simultaneously, update the access policy. Li *et al.*, [53] implemented a GRoup AKA (GRAKA) scheme with the Diffie-Hellman Key Exchange for Congestionless verification, Dynamically Updating Access rules and Session Key Establishment. Communicating devices authenticate simultaneously, update the access policy. GRAKA outdoes ASymmetric but not Symmetric Key Cryptography-based AKA protocols; It suffers from Signaling Congestion. Griffin *et al.*, [54] proposed Authenticated Key Exchange protocols; gained from coupling passwords with multiple Biometric Technology to combat Phishing and provide Mutual Authentication and data confidentiality. Users need not possess and manage Digital Certificates or understand the complexities of their use. Li *et al.*, [55] proposed a Certificate-less Signcryption (COS) method with less processing overhead in UnSigncryption. It does not require any Scalar Product Function during the online stage, hence appropriate with devices of limited resources. Recipient Identification is mandatory for offline and is vulnerable to a Private Key compromise attack. Premnath *et al.*, [56] showed a significant reduction in the cryptographic computational processing for IoT nodes using smaller Cryptographic Key sizes. The computational time required to calculate a Public Key Modulus in an IoT node linearly grows with the size of Key. The processing load for IoT nodes can reduce if the Public Key size selected depends on the time and budget-constrained adversary model. A dynamic and static Two-Way Authentication [57] exchanges Session Key to encrypt data resilient to Impersonation and Password Cracking attacks. It enhances Biometric-based security solutions by protecting from Forgery and Brute-Force attacks.

Xiong *et al.*, [58] used Binary Tree, Key Generation Center, and temporary secret disclosure resistance to protect external communication. It provides non-repudiation for remote communication using Certificate-less Encryption. The Key-Updating cost of KGC increases logarithmically with the number of Clients. This authentication protocol is provably secure. Porambage *et al.*, [59] proposed dual Multi-Secret Sharing protocols where the Key Derivations implicitly authenticate group members for securing multicast messages. But, it is relevant to single initiator many-responders and not for multi Initiator multi Responder. Many researchers, [55], [60], designed a method to enhance security by improving the Key Agreement protocol using Two-Level Keys to prevent various attacks. The comparisons of five different existing Key Management schemes are shown in Table III.

V. ACCESS CONTROL

An architecture model for restriction of access in the IoT system is as shown in Fig. 4. Ray *et al.*, [61] integrated Lightweight Cryptographic primitives and PUFs, in tags to achieve safe node detection. It ensures the Non-Repudiation and privacy protection of Users and the Networked RFID System. The computational speed is reasonable to realize in Radio Frequency Identification tags and prevent fake objects and cloning. Li *et al.*, [62] addressed the challenges of the massive access and proposed a Systematic Distributed Access Control framework with three distributed control components: Broker Level Control, Cluster Head Level Control and Traffic Conditional Utility Control to improve the overall network performance and deal with the dynamic network. An Optimal Control and Potential algorithms consider the device capacity limitation, flexibility, and feasibility of control algorithms. Oliveira *et al.*, [63] proposed a Network Admission Control solution that detects the node presence, verifies, validates, and discards invalid frames. It incorporates the AES Cryptographic Symmetric method to ensure the legitimacy of valid nodes and secure the transmission of data frames. Static Global Key reduces the handshake time. Global Key Updating generates a new one without resetting every node. Cryptographically derived Elliptic Curve based addresses consumes less energy than the methods without Global Key and resilient to forgery attack. While 6LoWPAN Neighbor Discovery (ND), is unimmune.

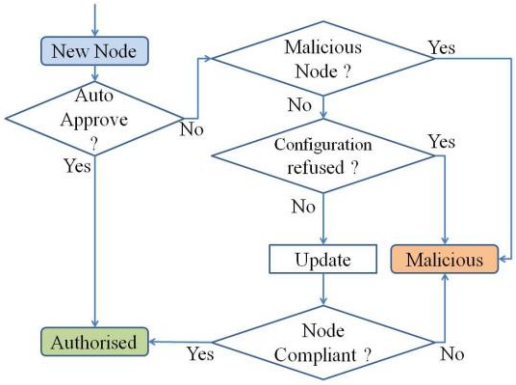

Fig. 4. Access Control in IoT

Saenko *et al.*, [64] presented a solution for reconfiguring the Admission protocols (Boolean Matrix Factorization) using an Improved Genetic Algorithm. The reconfiguration process utilizes an earlier Admission Management technique as input. Hu *et al.*, [65] proposed an efficient ABE and Signature scheme employing CPABE and stores signed data as Cipher. A Role-based Access Tree describes the access rights. The scheme is collusion resistance but increases storage requirements; Extra computation costs are in CPABE with multi-authority and constant Ciphertext length. Li *et al.*, [66] used Identity-based Cryptography to verify, validate, and allow the user to send information to a sensor. It has less computation cost and energy consumption. But the broker can create Congestion as Gateway's Authentication induces a computational overhead. Zhang *et al.*, [67] propound a D2D communication scheme using Certificate-Less Generalized SignCryption (CLGSC) and Chain of Hash functions. The CLGSC implemented with EC Discrete Logarithm Problem (DLP) without pairing reduces the execution cost. The encryption mode does not use exponentiation or pairing. The decryption uses single exponentiation.

Oh *et al.*, [68] devised a feasibility issue in maximizing the random access efficiency and designed a Joint Dynamic Access Control algorithm assessing a fluctuating number of communicating devices to reduce the effect on the efficiency by large and parallel admission endeavors.

Table- III: Key Management Schemes Summary

Article	Method	Advantage	Disadvantage
Castiglione *et al.*, [42]	hierarchical key assignment	Key uniformity with well-organized key generation and renewal schemes.	it requires every Client to accumulate only a distinct secret key
Raza *et al.*, [43]	Devices use DTLS with derived keys and authorized public keys.	Scalable in resource-constrained devices. Pre-provisioning of multiple pre-shared symmetric keys (PSKs) and out-of-band approval of public secrets are not required.	DoS attack can be injected by transmitting a greeting message and exploiting the session slots.
Li *et al.*, [44]	Heterogeneous Ring Signcryption	resistant to adaptive chosen cipher text attacks, adaptive chosen messages attacks with confidentiality, integrity, Authentication, non-repudiation, and anonymity.	consumes more energy
Li *et al.*, [53]	Non-concurrent key-share and DH session-key trade are collectively employed to provide distributed verification, validation, and secret-key utilization.	Less Bandwidth consumption. Authenticate several MTC devices simultaneously, dynamic renewal of admission rules, resistance to various typical attacks	Computational is less compared to symmetric cryptography always suffers from signaling Congestion
Li *et al.*, [55]	COS scheme	No arbitrary-point multiplication when Online; suitable for devices with limited resources	a recipient's individuality is a must when Offline.

Bouij-Pasquier *et al.*, [69] designed SmartOrBAC to enhance the ORganization-Based Access Control model. It divides the task into various service levels. The execution overhead spread among the devices of varying levels and limitations, along with measures to collective level issues. The single access policy access internally and externally. Security policy management enhances with reduced complexity and cost of administration of Access Control policies. An Authority Delegation manages the dynamic connection between Sensor and Resource/Client Authorized Engine. Fafoutis *et al.*, [70] focused on the plan and execution of the MAC layer of implanted devices controlled by Energy Harvesting (EH), which initiates a location ambiguity in the MAC layer of interactions that affect the execution time. On-Demand MAC is an Authentication scheme that depends on the recipient instigate the concept of contradictory interactions to handle the difficulties of EH exchanges. Yeh *et al.*, [71] used a variant of a CPABE, double encoding, and Merkle Hash Trees to support Strong Admission, Active Information and Group Inspection, Attribute Revocation. Access control uses the identity of devices to provide authorization to access data. The Access Trees, Vectors are used to maintain the Access policy.

A. Identity Management

In Batch Key Distribution [72] an instance creates and the secret share in a single step by applying the ID-Based Key Encapsulation method. With limited expenses, a single KGC allocates separate session keys to various nodes in the group. Confidential records can be uploaded by mobile Clients satisfying the security features. Saxena *et al.*, [73] designed an Authentication scheme to weaken the threats by validating the User Agreement and Authenticate the Client collectively every time a User contacts the node. The Client responsibility derives from an active Access Control. Two-Factor verification disables malicious devices to reuse data. Lo *et al.*, [74] introduced an Identity-based Batch Signature (IBS) scheme and a Signature System derived from ECC to develop a Conditional Privacy-Preserving Authentication scheme. IBS does not utilize any MapToPoint operation and pairing operation to increase efficiency in terms of time consumption. It outdoes Pseudo-ID-based Authentication. It supports verification of secret, data reliability, and group-secret Authentication.

Shim *et al.*, [75] adopted an Additive Homomorphic Encryption scheme to access the message only by the nodes that belong to a Cluster in the Data Aggregation process [76]. Non-paired Identity-based Signature scheme authentication, Batch verifier with Binary Quick Search used to decrease the computational cost of verifying many messages signed by various Sender signatures over MICAz and Tmote Sky. He *et al.*, [77] constructed a multi-Domain Contract mechanism using Hierarchical Cryptography. It is secure with the intractability of the Inversion CDH (ICDH) assumption. Witkovski *et al.*, [78] offered a Two-Key-based Authentication to incorporate Identity Management (IDM), which uses a Gateway to avoid the single point of compromise by using Symmetric Keys. It is a Single Sign-On with no overhead of communicating with an Internet Server. Open Authorization (OAuth) protocol [79] allows secure authorization invoking an external Authorization targeting HyperText Transfer Protocol / Constrained Application Protocol. It achieves low execution cost and extensibility. The resource utilized is more, as the information is divided into smaller units to fit into the standard packet format. The comparisons of five different existing Access Control schemes are shown in Table IV.

VI. SECURITY ATTACKS AND COUNTER MEASURES

The Threat detection identifies the known threats; the Active defense handles the Active attacks; Defensive strategies recognize and Handle the Active threats. The Recovery measures are proactive; Recovery schemes are preventive. A model for Proactive and Reactive strategies is as shown in Fig. 5. Indre *et al.*, [80] presented a Detection and Prevention system that understands the behavior of malicious network activities, detects and prevents infection *viz.*, Denial-of-Service (DoS), Probing, Address Resolution Protocol Spoofing, Distorted Packets, and Active Botnet. It extracts association from the packet history for the similar and dissimilar functionalities and nodes derived from the Rate of Rejection, header, and connection states.

Table- IV: Access Control Schemes

Article	Method	Advantage	Disadvantage
Ray *et al.*, [61]	simple cryptic functions and PUFs	secure, less computation cost, appropriate for cheaper RFID tags without the application dependency.	A specialized scheme collects the applicable data of the thing to guarantee framework knowledge.
Hu *et al.*, [65]	CPABE and signature	Role-based access, authenticated messages, and collusion resilience and are feasible.	There are extra computation costs and increased storage requirements.
Cirani *et al.*, [79]	OAuth-based authorization service	low execution cost, elegant admission strategies, and extensibility, no absolute functionality on the device.	energy consumption is more
Bouij-Pasquier *et al.*, [69]	enhanced the Organization-based Access Control	Single access policy access internally and externally; Security policy management enhance with reduced complexity. This model is extensive. The cost of administration of access control policies is reduced.	The applicability, validity and feasibility are not validated.

In a Protected Data Transmission [81], the arbitrarily distributed Listene interactsr. The possibility of compromising is calculated for the devices networked and having one Transmitter. The energy utilization and ratio of data and transmitted bits derive depending on the limitations of compromising the security. Appropriate indirect communication can increase the performance of device security and its range.

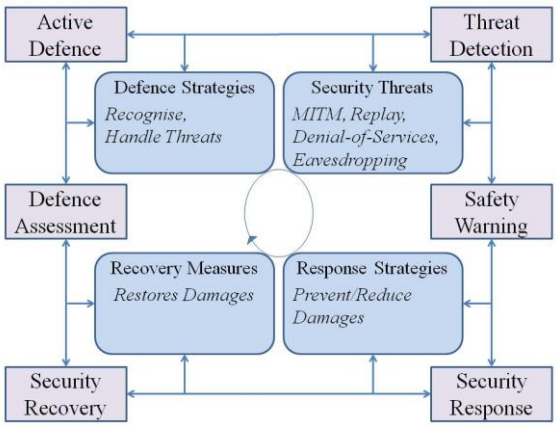

Fig. 5. Security Attacks and Countermeasures in IoT

Guan *et al.*, [82] searched the security patterns by processing the Knowledge obtained by a Conceptual method to maintain the safety characteristics, prototypes, and inter-associations. Sun *et al.*, [83] proposed malware detection with a large detection rate preserving privacy. A signature detection mechanism in suspicious bucket cross-filtering of the Server gives orientations of malicious Signature Fragments (SF). The SF digest in the scanning agent of the Client decreases the exact matching range. The interaction achieves confidentiality, and the modular Hash function reduces the communication cost. It provides malware detection and confidentiality with minor traffic and storage requirements. Tsimbalo *et al.*, [84] used employed Belief Propagation (BP), and Error Control Codes for an Iterative Decoding technique. A reduced number of retransmissions lead to longer battery life.

Mandal *et al.*, [85] introduced dual instances of Warbler PRNG with a Combination of revised De Bruijn for variable-length block and a Welch-Gong transformation for the filtration. PRNG is defiant to Cryptographic, *viz.*, mathematical, Black-box, Period-Storage-Information Trade-off, and Fault Injection attacks.

Dofe *et al.*, [86] analyzed the Applied Permutation to tackle a Hardware attack. Zhang *et al.*, [87] simulated a Double Hop wireless communication for Data Collection with non-collusion and M-collusion eavesdropper. The Eavesdropper collusion increases Secrecy Outage Performance (SOP) deteriorating secure data collection. The Cooperative Jamming scheme decreases SOP by allocating additional relays or increasing the noise generating threshold.

Giaretta *et al.*, [88] introduced two types of attacks: Black-hole, Sentry attacks, and proposed countermeasures. In a Black-hole attack, the decision process counters the threat, but, in a Sentry attack, only minimal computational capabilities are necessary. But, the decision process required to counter, dependent on the regions where emitted the attractants and the locations. Hossain *et al.*, [89] proposed a Secure Communication protocol with Facial Recognition and Functional Encryption as existing solutions provide no security in transmitting data between various Sensors and functionalities. Because of the uniqueness of traits, Biometric approaches are less exposed to attacks.

Bairagi *et al.*, [90] proposed Information Hiding techniques incorporating Shared Secret key and Dynamic positioning for protecting communication using an RGB image Steganographic approach. The opponent can be unable to analyze the original message. It achieved better resistance to Stego-only, Stego-cover, Visual, and Analysis attacks.

Fang *et al.*, [91] recognized a Virtual Multi-path attack from dissimilar locality methods derived from the spatial non-correlation. A fake multi-path medium deteriorates the locality of the Receiver, can discover and withstand using an assistant Receiver and detect the fake multi-path medium. This attack can modify specific path feature successfully.

Desnitsky *et al.*, [92] proposed a Detection of Deviated Data method to extract and use the proficient information. The analysis does not include erroneous, partial, and unpredicted data. Cervantes *et al.*, [93] designed an Invasion Identification scheme to recognize Sinkhole attacks on the Path-Discovery functionalities. The dynamic Clustering to carry out Data Communication examines the router behavior in retransmitting the data. Credibility mechanisms identify the behavior of doubtful routers.

Table-V: Security Attacks And Counter Measures Summary

Article	Method	Advantage	Disadvantage
Sun *et al.*, [83]	Signature-based malware detection mechanism using a formation of the restorable sketch.	Efficient malware detection; confidentiality with low communication cost.	The traffic and memory requirements are compromised.
Tsimbalo *et al.*, [84]	The Iterative Decoding technique is used for CRC error-correction	no extra overload for a transmitter.	It introduces complexity at the receiver side. Performance depends on iteration limit.
Zhang *et al.*, [87]	Two-hop wireless communication is incorporated to collect data i	Simple cooperative jamming is a physical layer security approach; a Security guarantee for the data collection	involves a high cost.
Giaretta *et al.*, [88]	black-hole, sentry attacks, and proposed its countermeasures	In a sentry attack, only minimal computational capabilities are required for the L-BNTs, which leads to simplicity, where random movements are sufficient to counter the threat.	A decision process is required to counter the black-hole attack that depends on regions where they have emitted the attractants and the locations of the M-BNTs.

Arias *et al.*, [94] analyzed that wearable devices compromise Boot Process vulnerabilities. The software cannot decide its legitimacy without the eligibility to validate itself. He *et al.*, [95] proposed a Pseudonym-based Near Field Communication (PNFC) protocol to remove vulnerabilities of the existing ones. PNFC provides Two-Way Validation, User Identification, Shared Secret Protection, and Forward Security and is resilient to Masquerading, Replay, MITM, and modification attacks. It provides stronger protections to NFC.

Chen *et al.*, [96] developed an Adaptable Filtering method to dynamically merge direct and indirect trust, reducing the execution time and biased assessment of having the compromised node with Strategic Functionality and Colluding attacks. This method enables each User to choose and use the feasible weight set, which causes a trustworthy response, reduces biased trust, and increases usability. The resource-constrained node maintains the trusted knowledge of interested nodes and further minimizes the trust renewal. Only persistent attackers are considered, and the member impetuses for Colluding attacks are unutilized.

Bhattacharyya *et al.*, [97] proposed an Agreement process during the Session Initialization by applying Two-level Communication. The communication process launch by the CoAP and the data transmission by the DTLS. It achieves resistance from IoT attacks *viz.*, Cipher, DoS, and Playback. It is feasible for one-to-one communication and cannot be suitable for one-to-many communication. Padmashree *et al.*, [98] proposed CKDAC that secures interaction in an IoT device cluster. The destructive node does not involve a network communication process. Various researchers [99], [100], proposed many methods to provide resistance against the attacks. Table V compares the existing Security Attacks and Counters.

VII. RESULT ANALYSIS

This paper provides a brief analysis of the existing methods, advantages, and limitations. Because of resource limitations, complex and robust security solutions with high security levels cannot be integrated into the IoT environment. The existing protocols designed for multiple layer security measures use Pseudonymous Certification, XoR, Hash, Nonces, ECC-based, EC-DH, ECDSA, Group Keys exchange. Two-way, three-factor authentication uses hierarchical derived private and public keys. PUFs, AES, Hybrid Ring encryption, CPABE, Attribute, Organization, Role, control Access with or without trusted Service Manager. Table VI shows the security approaches of various existing protocols. These protocols cannot authenticate in continuously evolving diverse environments. Most of the protocols are vulnerable to Brute Force, Replay, Black-hole, DoS, Collusion, Forgery, Impersonation attacks; cannot preserve User anonymity property; suffer from signaling Congestion. It consumes more energy, computation costs, storage requirements, response time delay, and network overhead.

Table-VI: Security measures

RSA	AES	ECC	XOR	HASH	NONCE
-	[3]	-	-	-	-
-	-	[4]	-	-	-
-	-	-	-	[11]	[11]
-	-	[15]	-	-	-
-	-	[19]	-	-	-
[20]	-	-	-	-	-
-	[21]	-	-	-	-
-	-	-	-	[22]	-
-	-	[30]	-	-	-
-	-	-	-	[32]	-
-	-	-	-	[33]	-
-	-	-	[34]	[34]	-
-	-	-	-	-	-
-	-	-	35]	[35]	[35]
-	-	-	-	-	[38]
-	-	-	-	-	[39]
[47]	-	-	-	-	-
-	-	-	-	[50]	-
-		[52]		[52]	
-	-	[67]	-	[67]	-
-	-	-	-	[71]	-
-	-	[74]	-	-	-
-	-	-	-	[83]	-
-	-	[98]	-	[98]	-
-	-	[100]	-	[100]	-

RSA provides a high-security level but more communication and computation cost. Most of the ECC-based Authentication schemes have acceptable attainment but are undefendable to all security breaches. Advanced Encryption Standards and the achieve authenticated Encryption with associated data but not suitable for restricted resource environment. Thus, the current requirement is for an efficient Access Control and Authentication with Key management that consider the complexity and energy limitations in security designs.

VIII. CONCLUSIONS

IoT involves a massive number of applications with intelligent objects that communicate on an interconnected platform based on the Internet. Many research includes wired and WSNs, MANETs, WBAN, RFID, Pervasive Computing. Due to the increasing implications of individuals or their gadgets in these applications, security concerns have turned into an unavoidable significant issue. Most protocols *viz.*, CoAP and MQTT are UDP-based (between Gateway and device) and hence incapable of protecting IoT Smart User application and IoT things laterally. The security challenges need to endeavor from the design stage to the IoT deployment to avoid intrinsic vulnerabilities associated with the Internet. Authentication and Access Control are essential protective strategies for preventing IoT devices and components from being victims of an attack. This review work primarily analyzed Authentication, Key Management, Access Control, and Malicious Node Detection techniques for a workable solution for the IoT. A novel strategy must secure a system with M2M devices installed for a longer duration with limited resources in IoT.

REFERENCES

1. A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–604, 2017.
2. N. Oualha, and K. T.Nguyen, "Lightweight Attribute-based Encryption for the Internet of Things," *in Proceedings of the 25th International Conference on Computer Communication and Networks*, pp. 1–6, 2016.
3. J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim, "Secure IoT Framework and 2D Architecture for End-To-End Security," *Journal of Supercomputing*, vol. 74, no. 8, pp. 3521–3535, 2018.
4. M. G. Padmashree, S. Khanum, J. S. Arunalatha, K. R. Venugopal, "SIRLC: Secure Information Retrieval using Lightweight Cryptography in HIoT," *in Proceedings of the IEEE International Technical Conference of Region 10 (TENCON 2019)*, pp. 169-173, 2019.
5. W. Aman, "Assessing the Feasibility of Adaptive Security Models for the Internet of Things," *in Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 201–211, 2016.
6. R. D. Chamberlain, M. Chambers, D. Greenwalt, B. Steinbrueck, and T. Steinbrueck, "Layered Security and Ease of Installation for Devices on the Internet of Things," *in Proceedings of the IEEE First International Conference on Internet-of-Things Design and Implementation*, pp. 297–300, 2016.
7. S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "Security, Privacy & Incentive Provision for Mobile Crowd Sensing Systems," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 839 – 853, 2016.
8. H. Ye, J. Yang, J. Zhu, Z. Zhang, and Y. Huang, "A Secure Privacy Data Transmission Method for Medical Internet of Things," *in Proceedings of IEEE International Conference on Industrial IoT Technologies and Applications*, vol. 173, pp. 144–154, 2016.
9. M. Tiloca, C. Gehrmann, and L. Seitz, "On Improving Resistance to Denial of Service and Key Provisioning Scalability of the DTLS Handshake," *International Journal of Information Security*, vol. 16, no. 2, pp. 173–193, 2016.
10. G. Alpár, L. Batina, L. Batten, V. Moonsamy, A. Krasnova, A. Guellier, and I. Natgunanathan, "New Directions in IoT Privacy Using Attribute-Based Authentication," *in Proceedings of ACM International Conference on Computing Frontiers*, pp. 461–466, 2016.
11. K. H. Han and W. S. Bae, "Proposing and Verifying a Security Protocol for Hash Function-Based IoT Communication System," *Cluster Computing*, vol. 19, no. 1, pp. 497–504, 2016.
12. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF Enabled Secure Architecture for FPGA-Based IoT Applications," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 110–122, 2015.
13. S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-End Security Scheme for Mobility Enabled Healthcare Internet of Things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, 2015.
14. J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a Lightweight Authentication and Authorization Framework for Smart Objects," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 4, pp. 690–702, 2015.
15. P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," *IEEE Sensors Journal*, vol. 15, no. 9, pp. 5340–5348, 2015.
16. G. C. Polyzos and N. Fotiou, "Building a reliable Internet of Things using Information-Centric Networking," *Journal of Reliable Intelligent Environments*, vol. 1, no. 1, pp. 47–58, 2015.
17. H. Zhang and T. Zhang, "A Peer to Peer Security Protocol for the Internet of Things": Secure Communication for the Sensible Things Platform," *in Proceedings of the 18th International Conference on Intelligence in Next Generation Networks*, pp. 154–156, 2015.
18. S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, "A Security-And Quality-Aware System Architecture for Internet of Things," *Information Systems Frontiers*, vol. 18 pp. 665–677, 2016.
19. Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 237–248, 2017.
20. D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 72–83, 2015.
21. D. Chakraborty and P. Sarkar, "On Modes of Operations of a Block Cipher for Authentication and Authenticated Encryption," *Cryptography and Communications*, vol. 8, no. 4, pp. 455–511, 2016.
22. S. Jang, D. Lim, J. Kang, and I. Joe, "An Efficient Device Authentication Protocol Without Certification Authority for Internet of Things," *Wireless Personal Communications*, vol. 91, no. 4, pp. 1681–1695, 2016.
23. M. N. Aman, K. C. Chua, and B. Sikdar, "Position Paper: Physical Unclonable Functions for IoT Security," *in Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pp. 10–13, 2016.
24. Tian, X. Chen, D. Guo, J. Sun, L. Liu, and J. Hong, "Analysis and Design of Security in Internet of Things," *in Proceedings of the 8th International Conference on BioMedical Engineering and Informatics*, no. 8, pp. 678–684, 2016.
25. F. Wu, L. Xu, S. Kumari, and X. Li, "A Privacy-Preserving and Provable User Authentication Scheme for Wireless Sensor Networks Based on Internet of Things Security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101–116, 2017.
26. L. Lu and Y. Liu, "Safeguard: User Reauthentication on Smartphones via Behavioral Biometrics," *IEEE Transactions on Computational Social Systems*, vol. 2, no. 3, pp. 53–64, 2016.
27. Giri, R. Sherratt, and T. Maitra, "A Novel and Efficient Session Spanning Biometric and Password-Based Three-Factor Authentication Protocol for Consumer USB Mass Storage Devices," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 3, pp. 283–291, 2016.
28. P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124–7132, 2016.
29. J. R. Wallrabenstein, "Practical and Secure IoT Device Authentication Using Physical Unclonable Functions," *in Proceedings of 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 99–106, August 2016.
30. P. Gasti, J. Sedenka, Q. Yang, G. Zhou, and K. Balagani, "Secure, Fast, and Energy-Efficient Outsourced Authentication for Smartphones," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2556 – 2571, 2016.
31. G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang, and S. Wang, "Continuous Authentication With Touch Behavioral Biometrics and Voice on Wearable Glasses," *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 3, pp. 404–416, 2017.
32. R. Amin, H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an Anonymity-Preserving Three-Factor Authenticated Key Exchange Protocol for Wireless Sensor Networks," *Computer Networks*, vol. 101, pp. 42–62, June 2016.

33. S. Arasteh, S. F. Aghili, and H. Mala, "A New Lightweight Authentication and Key Agreement Protocol for Internet of Things," *in Proceedings of the 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, pp. 52–59, September 2016.
34. M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An Efficient User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Network Tailored for the Internet of Things Environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2015.
35. H. Khemissa and D. Tandjaoui, "A Novel Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things," *in Proceedings of Wireless Telecommunications Symposium (WTS)*, pp. 1–6, April 2016.
36. H. Ren, Y. Song, S. Yang, and F. Situ, "Secure Smart Home: A Voiceprint and Internet-Based Authentication System for Remote Accessing," *in Proceedings of the 11th International Conference on Computer Science & Education*, pp. 247–251, 2016.
37. C. Chang and H. Le, "A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357–366, 2016.
38. A. Ceccarelli, L. Montecchi, F. Brancati, P. Lollini, A. Marguglio, and A. Bondavalli, "Continuous and Transparent User Identity Verification for Secure Internet Services," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 3, pp. 270–283, 2015.
39. R. Giuliano, F. Mazzenga, A. Neri, and A. M. Vegni, "Security Access Protocols in IoT Capillary Networks," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 645–657, 2017.
40. 58. C. Gehrmann, M. Tiloca, and R. Hoglund, "SMACK: Short Message Authentication Check Against Battery Exhaustion in the Internet of Things," *in Proceedings of the 12th Annual IEEE International Conference on Sensing, Communication, and Networking*, pp. 274–282, June 2015.
41. M. A. Iqbal and M. Bayoumi, "Secure End-to-End Key Establishment Protocol for Resource-Constrained Healthcare Sensors in the Context of IoT," *2016 International Conference on High-Performance Computing Simulation*, pp. 523–530, 2016.
42. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, and X. Huang, "Cryptographic Hierarchical Access Control for Dynamic Structures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2349–2364, 2016.
43. S. Raza, L. Seitz, D. Sitenkov, and G. Selander, "S3K: Scalable Security With Symmetric Keys - DTLS Key Establishment for the Internet of Things," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1270–1280, 2016.
44. F. Li, Z. Zheng, and C. Jin, "Secure and Efficient Data Transmission in the Internet of Things," *Telecommunication Systems*, vol. 62, no. 1, pp. 111–122, 2016.
45. Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 29–39, 2017.
46. M. A. Iqbal and M. Bayoumi, "A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource-Constrained Body Area Sensors," *in Proceedings of IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 315–320, Aug 2016.
47. J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, "High-Performance and Lightweight Lattice-Based Public-Key Encryption," *in Proceedings of the Second ACM International Workshop on IoT Privacy*, Trust, and Security, pp. 2–9, 2016.
48. Barki, A. Bouabdallah, S. Gharout, and J. Traoré, "M2M Security: Challenges and Solutions," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1241–1254, 2016.
49. Y. Qiu and M. Ma, "A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2074–2085, 2016.
50. H. Ning, H. Liu, and L. T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 657–667, 2015.
51. M. A. S. Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and Escrow-Less Authenticated Key Agreement for the Internet of Things," *Computer Communications*, vol. 98, pp. 43–51, 2016.
52. M. G. Padmashree, J. S. Arunalatha, K. R. Venugopal, "HPAKE: Hybrid Precocious Authentication and Key Establishment in IoT," *in Proceedings of the IEEE FiftyThird International Carnahan Conference on Security Technology (ICCST 2019)*, pp. 129-134, 2019.
53. J. Li, M. Wen, and T. Zhang, "Group-Based Authentication and Key Agreement with Dynamic Policy Updating for MTC in LTE-A Networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408 – 417, 2015.
54. P. H. Griffin, "Security for Ambient Assisted Living: Multi-factor Authentication in the Internet of Things," *in Proceedings of IEEE Globecom Workshops*, pp. 1–5, 2015.
55. F. Li, Y. Han, and C. Jin, "Certificateless Online/Offline Signcryption for the Internet of Things," *Wireless Networks*, vol. 23, no. 1, pp. 145–158, 2017.
56. S. N. Premnath and Z. J. Haas, "Security and Privacy in the Internet-of-Things under Time-and-Budget-Limited Adversary Model," *IEEE Wireless Communications Letters*, vol. 4, no. 3, pp. 277–280, 2015.
57. Giri, R. S. Sherratt, T. Maitra, and R. Amin, "Efficient Biometric and Password-Based Mutual Authentication for Consumer USB Mass Storage Devices," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 4, pp. 491–499, 2015.
58. H. Xiong and Z. Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1442–1455, 2015.
59. P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications," *IEEE Access*, vol. 3, pp. 1503–1511, 2015.
60. R. Tanuja, S. H. Manjula, K. R. Venugopal, and L. M. Patnaik, "Secure and Privacy Preserving Data Centric Sensor Networks With Multi-Query Optimization," *IJRET: International Journal of Research in Engineering and Technology*, vol. 04, no. 01, pp. 247–254, Jan 2015.
61. R. Ray, M. U. Chowdhury, and J. H. Abawajy, "Secure Object Tracking Protocol for the Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 544–553, 2016.
62. Y. Li, K. K. Chai, Y. Chen, and J. Loo, "Distributed Access Control Framework for IPv6-Based Hierarchical Internet of Things," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 17–23, 2016.
63. L. M. Oliveira, J. J. P. C. Rodrigues, A. F. De Sousa, and V. M. Denisov, "Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2186–2195, 2016.
64. Saenko and I. Kotenko, "Reconfiguration of Access Schemes in Virtual Networks of the Internet of Things by Genetic Algorithms," *Intelligent Distributed Computing IX: in Proceedings of the 9th International Symposium on Intelligent Distributed Computing – IDC'2015,* pp. 155–165, October 2016.
65. Hu, H. Li, and Y. Huo, "Secure and Efficient Data Communication Protocol for Wireless Body Area Networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.
66. F. Li, Y. Han, and C. Jin, "Practical Access Control for Sensor Networks in the Context of the Internet of Things," *Computer Communications*, vol. 89, pp. 154–164, 2016.
67. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2017.
68. Y. Oh, D. Hwang, and T. J. Lee, "Joint Access Control and Resource Allocation for Concurrent and Massive Access of M2M Devices," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4182–4192, 2015.
69. Bouij-Pasquier, A. A. Ouahman, A. A. E. Kalam, and M. Ouabiba de Montfort, "SmartOrBAC Security and Privacy in the Internet of Things," *in Proceedings of IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–8, Nov 2015.
70. X. Fafoutis, A. D. Mauro, C. Orfanidis, and N. Dragoni, "Energy-Efficient Medium Access Control for Energy Harvesting Communications," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 4, pp. 402–410, 2015.
71. L. Y. Yeh, P. Y. Chiang, Y. L. Tsai, and J. L. Huang, "Cloud-based Fine-grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation," *IEEE Transactions on Cloud Computing*, vol. 6 , no. 2, pp. 532 - 544, 2015.
72. W. Wang, P. Xu, L. T. Yang, and J. Chen, "Cloud-Assisted Key Distribution in Batch for Secure Real-time Mobile Services," *IEEE Transactions on Services Computing*, vol. 11, no. 5, pp. 850 - 863, 2018.

73. N. Saxena, B. J. Choi, and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907–921, 2016.
74. N. W. Lo and J. L. Tsai, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.
75. K. A. Shim and C. M. Park, "A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2128–2139, 2015.
76. L. González-Manzano, J. M. de Fuentes, S. Pastrana, P. Peris-Lopez, and L. Hernández-Encinas, "PagIoT: Privacy-Preserving Aggregation Protocol for Internet of Things," *Journal of Network and Computer Applications*, vol. 71, pp. 59–71, 2016.
77. D. He, N. Kumar, H. Wang, L. Wang, K. K. R. Choo, and A. Vinel, "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 633 - 645, 2018.
78. Witkovski, A. Santin, V. Abreu, and J. Marynowski, "An IdM and Key-based Authentication Method for providing Single Sign-On in IoT," *in Proceedings of the IEEE Global Communications Conference (GLOBECOM-2015)*, pp. 1–6, 2015.
79. S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoTOAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 1224–1234, 2015.
80. Indre and C. Lemnaru, "Detection and Prevention System against Cyber Attacks and Botnet Malware for Information Systems and Internet of Things," *in Proceedings of the IEEE 12th International Conference on Intelligent Computer Communication and Processing*, pp. 175–182, 2016.
81. Q. Xu, P. Ren, H. Song, and Q. Du, "Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations," *IEEE Access Special Section on Internet of Things (IoT) in 5G Wireless Communications*, vol. 4, pp. 2840–2853, 2016.
82. H. Guan, H. Yang, and J. Wang, "An Ontology-Based Approach to Security Pattern Selection," *International Journal of Automation and Computing*, vol. 13, no. 2, pp. 168–182, 2016.
83. H. Sun, X. Wang, R. Buyya, and J. Su, "CloudEyes: Cloud-Based Malware Detection with Reversible Sketch for Resource-Constrained Internet of Things (IoT) Devices," *Software: Practice and Experience*, vol. 47, no. 3, pp. 421–441, 2017.
84. Tsimbalo, X. Fafoutis, and R. J. Piechocki, "CRC Error Correction in IoT Applications," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 361–369, 2017.
85. K. Mandal, X. Fan, and G. Gong, "Design and Implementation of Warbler Family of Lightweight Pseudorandom Number Generators for Smart Devices," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 15, no. 1, pp. 1–28, 2016.
86. J. Dofe, J. Frey, and Q. Yu, "Hardware Security Assurance in Emerging IoT Applications," *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 2050–2053, 2016.
87. Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On Secure Wireless Communications for IoT Under Eavesdropper Collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, 2016.
88. Giaretta, S. Balasubramaniam, and M. Conti, "Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 665–676, 2016.
89. M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward End-to-End Biometrics -Based Security for IoT Infrastructure," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 44–51, 2016.
90. K. Bairagi, R. Khondoker, and R. Islam, "An Efficient Steganographic Approach for Protecting Communication in the Internet of Things (IoT) Critical Infrastructures," *Information Security Journal: A Global Perspective*, vol. 25, no. 4-6, pp. 197– 212, 2016.
91. S. Fang, Y. Liu, W. Shen, H. Zhu, and T. Wang, "Virtual Multipath Attack and Defense for Location Distinction in Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 566–580, 2017.
92. V. A. Desnitsky, I. V. Kotenko, and S. B. Nogin, "Detection of Anomalies in Data for Monitoring of Security Components in the Internet of Things," *in Proceedings of International Conference on Soft Computing and Measurements*, pp. 189–192, 2015.
93. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things," *in Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management*, pp. 606–611, 2015.
94. O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, 2015.
95. He, N. Kumar, and J. H. Lee, "Secure Pseudonym-Based near Field Communication Protocol for the Consumer Internet of Things," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 1, pp. 56–62, 2015.
96. R. Chen, J. Guo, and F. Bao, "Trust Management for SoA-Based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482 – 495, 2015.
97. Bhattacharyya and Abhijan, "LESS: Lightweight Establishment of Secure Session: A Cross-Layer Approach Using CoAP and DTLSPSK Channel Encryption," *in Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, vol. 29, pp. 682–687, 2015.
98. M. G. Padmashree, Ranjitha, J. S. Arunalatha, K. R. Venugopal, "CKDAC: Cluster-Key Distribution and Access Control for Secure Communication in IoT," *in Proceedings of the Seventh IEEE Uttar Pradesh Section International Conference on Electrical*, Electronics and Computer Engineering (UPCON 2020), pp. 1-6, 2020.
99. M. G. Padmashree, J. S. Arunalatha, and K. R. Venugopal, "HSSM: High Speed Split Multiplier for Elliptic Curve Cryptography in IoT," *in Proceedings of the Fifteenth IEEE International Conference on Information Processing (ICInPro-2019)*, pp. 123-127, 2019.
100. M. G. Padmashree, S. Khanum, J. S. Arunalatha, and K. R. Venugopal, "ETPAC: ECC based Trauma Plight Access Control for Healthcare Internet of Things," Springer International Journal of Information Technology, vol. 13, no. 4, pp. 1481–1494, 2021.

AUTHORS PROFILE

M. G. Padmashree, received the B.E. Degree in Computer Science & Engineering from JNNCE, Shivamogga, Kuvempu University, Karnataka, India, in 1998 and the M.Tech. Degree in Computer Science & Engineering from RVCE, Visvesvaraya Technological University, Karnataka, in 2011. She is currently pursuing a Ph.D. degree in Computer Science and Engineering at Bangalore University, Bengaluru, India. She was working in Engineering Colleges with 17 years of teaching experience. She has published 6 articles in refereed International Journals and Conferences. Her research interest includes Scheduling, Operating Systems, Cryptography, Security in IoT.

J S Arunalatha, is a Professor in the Department of Computer Science and Engineering at University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. She obtained her Bachelor of Engineering in Computer Science and Engineering from PES College of Engineering, Mandya, Mysore University. She received her Master's degree in Computer Science and Engineering from Bangalore University. She pursued her Ph.D. program in the area of Biometrics. She has published 17 articles in refereed International Journals and conferences; Her research interest is in Biometrics, Image Processing, IoT, Big Data Analytics, and Web Mining.

K R Venugopal, is currently the Vice-Chancellor of Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science, and Journalism. He has authored and edited 77 books and has over 980 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing, Data Mining, IoT, and Cloud Computing. He received IEEE Fellow and ACM Distinguished Educator award from USA for his outstanding contributions to Computer Science and Engineering.