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.
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 confine 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 prevents 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.
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 CPAE. 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 communication overhead. The usage of the device increases across contrast sessions. It has relatively less computational and communication overhead.

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. Gashi 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.
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 None [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.
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.

Iqbal et al., [46] designed an AKA protocol resistant 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. Je et al., [51] analyzed the agreement without CA and showed that the Strengthened-Menezes-Qu- VANstone and Implicit Certificates improve 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 GRow-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 GReoup 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 outperforms 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 immune.

![Fig. 4. Access Control in IoT](image)

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] proposed 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.
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 collect 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>
<thead>
<tr>
<th>Article</th>
<th>Method</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Castiglione et al., [42]</td>
<td>Hierarchical key assignment</td>
<td>Key uniformity with well-organized key generation and renewal schemes.</td>
<td>It requires every Client to accumulate only a distinct secret key.</td>
</tr>
<tr>
<td>Raza et al., [43]</td>
<td>Devices use DTLS with derived keys and authorized public keys.</td>
<td>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.</td>
<td>DoS attack can be injected by transmitting a greeting message and exploiting the session slots.</td>
</tr>
<tr>
<td>Li et al., [44]</td>
<td>Heterogeneous Ring Signcryption</td>
<td>Resistant to adaptive chosen cipher text attacks, adaptive chosen messages attacks with confidentiality, integrity, Authentication, non-repudiation, and anonymity.</td>
<td>Consumes more energy.</td>
</tr>
<tr>
<td>Li et al., [53]</td>
<td>Non-concurrent key-share and DH session-key trade are collectively employed to provide distributed verification, validation, and secret-key utilization.</td>
<td>Less Bandwidth consumption. Authenticate several MTC devices simultaneously, dynamic renewal of admission rules, resistance to various typical attacks.</td>
<td>Computational is less compared to symmetric cryptography always suffers from signaling Congestion</td>
</tr>
<tr>
<td>Li et al., [55]</td>
<td>COS scheme</td>
<td>No arbitrary-point multiplication when Online; suitable for devices with limited resources.</td>
<td>A recipient’s individuality is a must when Offline.</td>
</tr>
</tbody>
</table>
Table IV: Access Control Schemes

<table>
<thead>
<tr>
<th>Article</th>
<th>Method</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ray et al., [61]</td>
<td>simple cryptic functions and PUFs</td>
<td>secure, less computation cost, appropriate for cheaper RFID tags without the application dependency.</td>
<td>A specialized scheme collects the applicable data of the thing to guarantee framework knowledge.</td>
</tr>
<tr>
<td>Hu et al., [65]</td>
<td>CPABE and signature</td>
<td>Role-based access, authenticated messages, and collusion resilience and are feasible.</td>
<td>There are extra computation costs and increased storage requirements.</td>
</tr>
<tr>
<td>Cirani et al., [79]</td>
<td>OAuth-based authorization service</td>
<td>low execution cost, elegant admission strategies, and extensibility, no absolute functionality on the device.</td>
<td>energy consumption is more</td>
</tr>
<tr>
<td>Bouji-Pasquier et al., [69]</td>
<td>enhanced Organization-based Access Control</td>
<td>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.</td>
<td>The applicability, validity and feasibility are not validated.</td>
</tr>
</tbody>
</table>

In a Protected Data Transmission [81], the arbitrarily distributed Listene interactors. 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.

Doe, 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.

Baragi 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.
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.

<table>
<thead>
<tr>
<th>Article</th>
<th>Method</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun et al., [83]</td>
<td>Signature-based malware detection mechanism using a formation of the</td>
<td>Efficient malware detection; confidentiality with low communication cost.</td>
<td>The traffic and memory requirements are compromised.</td>
</tr>
<tr>
<td>Tsimbalo et al.,</td>
<td>The Iterative Decoding technique is used for CRC error-correction</td>
<td>No extra overload for a transmitter.</td>
<td>It introduces complexity at the receiver side.</td>
</tr>
<tr>
<td>[84]</td>
<td></td>
<td></td>
<td>Performance depends on iteration limit.</td>
</tr>
<tr>
<td>Zhang et al., [87]</td>
<td>Two-hop wireless communication is incorporated to collect data i</td>
<td>Simple cooperative jamming is a physical layer security approach; a Security guarantee for the data collection</td>
<td>Involves a high cost.</td>
</tr>
<tr>
<td>Giaretta et al.,</td>
<td>black-hole, sentity attacks, and proposed its countermeasures</td>
<td>In a sentity attack, only minimal computational capabilities are required for the L-BNTs, which leads to simplicity, where random movements are sufficient to counter the threat.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>RSA</th>
<th>AES</th>
<th>ECC</th>
<th>XOR</th>
<th>HASH</th>
<th>NONCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>[3]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[15]</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[30]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>[20]</td>
<td>-</td>
<td>[21]</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>[30]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[32]</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[35]</td>
<td>[33]</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[34]</td>
<td>[34]</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>[35]</td>
<td>[35]</td>
<td>[35]</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[38]</td>
<td>[39]</td>
</tr>
<tr>
<td>[47]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[50]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>[52]</td>
<td>-</td>
<td>[52]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>[67]</td>
<td>-</td>
<td>[67]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[71]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>[83]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>[98]</td>
<td>-</td>
<td>[98]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>[100]</td>
<td>-</td>
<td>[100]</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

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 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 protecive 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


52. M. G. Padmashree, J. S. Aranalatha, K. R. Venugopal, “HPAKE: Hybrid Preco...
AUTHORS PROFILE

J S Arunalatha, is a Professor in the Department of Computer Science and Engineering at Bangalore University, Bengaluru, India. She has received her Master’s degree in Computer Science and Engineering from Bengaluru University. She has published over 13 articles in refereed International Journals and conferences; Her research interest includes Biometrics, Image Processing, IoT, Big Data Analytics, and Web Mining.

K R Venugopal, is currently the Vice-Chancellor of Bangalore University, Bangalore. He was born in Bangalore, Karnataka, India. He obtained his Ph.D. in Computer Science from the Indian Institute of Science, Bangalore. He is a distinguished academic and has degrees in Computer Science, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science, and Journalism. He has authored over 20 books and has over 900 research papers in 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 has received several awards for his outstanding contributions to Computer Science and Engineering.

M. G. Padmasree, received the B.E. degree in Computer Science & Engineering from JNNEC, Shimavogga, 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 PhD 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 interests include Scheduling, Operating Systems, Cryptography, Security in IoT.