RESEARCH ARTICLE OPEN ACCESS

Analysis on Lightweight Security Protocols for IoT Services

[1] K. Pushpalatha, Research Scholar, [2] Dr.R. Kalaiarasi, Assistant Professor

SOCS, TNOU - CHENNAI

ABSTRACT

Internet-of-Things (IoT) devices are solicited ubiquitously around the world due to their assorted applicability. The applications range from home automations office automations, industrial automations, control system automations, environmental sensing, natural resource consumption monitoring, traffic automations, pollution monitoring, waste managements, grid controlling, human healthcare, autonomous driving, smart agriculture and entire smart city control systems. Due to the versatility of the applications, the IoT network is vulnerable for many types of attacks. Since the IoT devices are extremely heterogeneous in software and hardware configurations, combining under one roof is a challenging task in which most of the researches are going about. This work is scalloped to uncover different types of latest IoT network protocols their benefits and the security issues against different types of attacks. Most recent research works regarding IoT security are carefully studied here to present a clear averment by analyzing the methodologies, their advantages and their limitations behind them. A conspicuous statement about the enhancements of the existing works and the need to develop new methodologies to strengthen the security of the IoT network environments are derived in this work.

Keywords: Internet-of-Things (IoT), Remote monitoring and automations, Security schemes, wireless network Protocols, Security Protocols, Network attacks.

I. INTRODUCTION

The term IoT refers that the physical objects with sensors, data handling ability and to communicate with other devices through direct internet or through other communication modes to exchange data among [1]. There are several developments brought out for decades such as edge and fog computing. An IoT device is typically an electronic device with optional sensors and actuators that could operate based on a software and can communicate with other devices mostly through IEEE 802.11 b/g/n protocol [2]. IoT devices are used globally for multiple applications in various fields. There are around 21.7 billion active connected devices in the current year 2024 and there are 11.7 billion devices are IoT devices. The ratio shows that the utilization of IoT is more than 54% in the entire active connected devices [3].

There are different types of IoT devises in which the most notable categories are Consumer IoT, Commercial IoT, Military Things (IoMT), Industrial IoT (IIoT) and Infrastructure IoT [4]. The Consumer IoT devices are used in home appliances, voice-assistance, smart home automations, and personal healthcare. Commercial IoT devices are used to professional healthcare monitoring systems and in Transport industries. IoMT devices are used for military usages such as in automated security devices, drones, surveillance robots and human wearable combat biometric devices. The primary use of IIoT devices are Industrial automations, Autonomous digital control systems, Manufacturing and Energy sector monitoring. Infrastructure IoT devices are mostly used in smart city resource managements [5].

IoT architecture natural inherits most of the properties of conventional wireless communication networks. There are several IoT Cyber security attacks are in practice these days those can be covered under the categories for instance Physical Attacks, Encryption Attacks, Denial of Service (DoS), Firmware hijacking, Botnets, Man-in-the-Middle attacks, Ransomware attacks, Eavesdropping attacks, Privilege Escalation attacks and Brute force Password attacks [6]. Based on the observed IoT network basics and advancements it is understood that a clear study about the attacks and the protection methods in the filed of IoT is required to enhance the security performance furthermore. The up-to-date available security models and protocols to prevent IoT networks against the above-mentioned attacks are discussed in this work.

II. EXISTING METHODS

Most recent Lightweight security protocols for IoT related services are selected to explore here to understand the elementary components, methodologies, advantages and their limitations. Many research articles from 2022 to till data are collected and befitting works are discussed elaborately in this section.

2.1. Securing End-Node to Gateway Communication on LoRaWAN with a lightweight security protocol [SEGCLLSP]

In 2022, Jhonattan J. Barriga et.al. introduced SEGCLLSP [7] work for the purpose of protecting LoRaWAN environments against authentication attacks by introducing lightweight cryptographic functions. SEGCLLSP work mainly concentrates on the security principles such as Confidentiality, Integrity and Availability. A detailed narration is provided about the real-time LoRaWAN security issues such as Bit-flipping attacks, channel eavesdropping rogue gateway attacks, mitigating gateway attack, ACK spoofing, Jamming attack, Beacon attack, Relay attacks and wormhole attack in SEGCLLSP work. A dedicated threat model is used in SEGCLLSP to evaluate the security of the communication between the End-Node and the Gateway. A dedicated set of protocols such as Gateway registration protocol, Gateway session key derivation protocol, Uplink messages over authenticated End-Nodes to Gateway protocol, and Uplink messages over unauthorized End-Nodes to Gateway protocol are introduced in SEGCLLSP work.

The security of SEGCLLSP method is proved through two different ways. The first one is a theoretical proof using BAN logic and the second one is using the Scyther tool. Communication overhead, power consumption and processing time are the parameters measured during the SEGCLLSP experiments. Achievement of better processing speed with lower power consumption and communication overhead is the achievement of SEGCLLSP. Measurement of security is only proved through BAN logic and a decade old evaluation tool is understood as the limitation of SEGCLLSP work. Most important parameters such as throughput, communication delays, and packet delivery ratio are not included during the evaluation of SEGCLLSP, which is also observed as the limitation of SEGCLLSP.

2.2. LR-AKAP: A Lightweight and Robust Security Protocol for Smart Home Environments

In 2022, Haseeb-ur-rehman RMA et.al., introduced LR-AKAP [8] work for smart home authentication security. It is stated that the LR-AKAP work protects smart homes from well-known attacks. A symmetric key based authentication protocol is introduced in LR-AKAP work to protect smart devices in a smart home. The security performance is measured using the AVISPA tool. Clock synchronization issue of timestamp-based two-way authentication protocols is clearly addressed in the LR-AKAP work. Initialization process, Device enrollment process, Gateway node enrollment process, User enrollment process, Login and Authentication process, Biometric and Password update process are certainly defined in LR-AKAP work. Security against popular attacks such as replay attack, session key attack, impersonation attack, man-in-the-Middle attack. computational cost, processing time, and security parameters are measured during the experiment process of LR-AKAP work. The computational overhead is measured for hash function, ECC multiplication, symmetric encryption process, decryption process and for bilinear pairing process individually during the experiment. The accumulation of these computational overheads is a little more than the compared existing works.

Improved security is the main advantage of LR-AKAP work, whereas slightly increased computational overhead can be a little difficult process for the battery operated IoT devices, which is the observed limitation. Vital network parameters such as communication delays and data transfer rate are not measured during the experiments.

2.3. Light-Weight Security Protocol and Data Model for Chip-to-Chip Zero-Trus [LSPDM]

A. Ahmed submitted et.al., Introduced LSPDM work in 2023 for the purpose of establishing Chip-to-Chip (C2C) communication at Zero-Trust (ZT) architecture. The motivation of LSPDM work is to provide a chip level authentication technique in ZT environment before establishing data communication. LSPDM method works on physical layer to achieve the security in C2C ZT environment. A dedicated algorithm to establish communication between the host chip and the external chip is provided in LSPDM work to overcome some IoT attacks such as Distributed Denial of Service (DDoS), Malware propagation, Replay attack, Zero-day exploits, Dataflow sniffing, and Collision attacks. The performance of LSPDM work is measured by using High-Level Protocol Specification Language (HLPSL) and AVISPA protocol evaluation tool. The AVISPA tool provides the security information into three categories such as safe, unsafe or inconclusive. By calculating the averages of there categories for different timestamps, the overall security is computed.

Achievement of security in C2C ZT Environment is the stated advantage of LSPDM work. At the same time, there are several security

protocols with Elliptic Curve Cryptography and Digital Certificate are in practice which provides competitive security levels. Missing measurements such as throughput and communication delays for multiple C2C communication for a continuous operative real-time environment or in a simulated environment during the experiments is the limitation of LSPDM. Lacking measurements of these vital network performance parameters is also understood as the limitation of LSPDM work.

2.4. A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things (LEAEWSN)

Ntebatseng Mahlake et.al., proposed LEAEWSN work in 2022 to address the complications of security issues and computational complexities in IoT services. In LEAEWSN work, the authors substitute lesser computational complication operations such as XOR and XNOR instead of conventional exponential numerical calculations. LEAEWSN uses a dedicated key expansion mechanism for encoding and decoding the keys. The keys are converted to a fixed length of 64-bits in LEAEWSN for ease of operation. This scaling process also used to maintain the balance between low and high security keys. After the key expansion process, the 64-bit keys are divided into nibbles (4-bits) and fed to the f-0function This specialized f-function has dedicated diffusion and confusion functionalities as given in Figure 1.

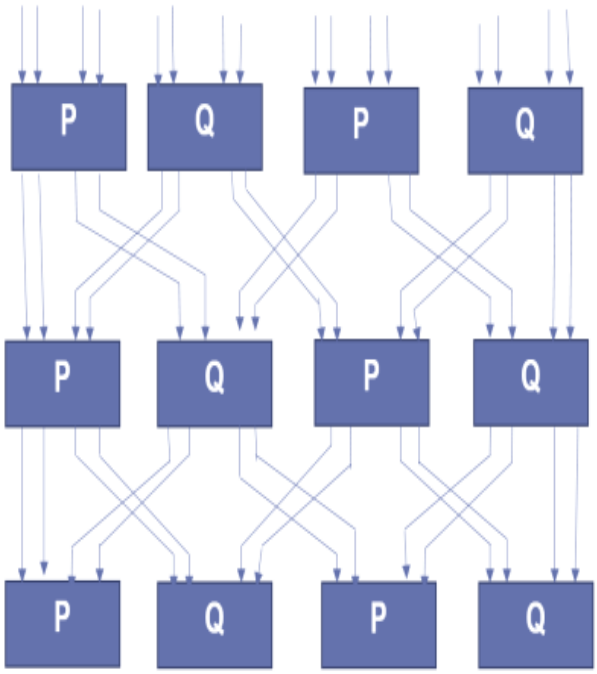

Figure 1: LEAEWSN f-function diffusion and confusion

Then the diffused keys are grouped into 16-bit arrays to provide round keys. Similarly customized key management method and encryption methods are introduced in LEAEWSN work to provide security for the IoT services.

The experiments are carried out using MATLAP 2022a using IEEE 802.11 simulation. The simulation environment is set to be a 00x400 square meter area with 100 number of nodes at random clustered distribution-based placement. Parameters such as security, energy consumption, key expansion time and packet delivery ratio are measured during the experiments.

Achievement of higher Security higher packet delivery ratio and lower energy consumption are the achievements of LEAEWSN work Most important IoT network evaluation metrics such as Throughput, End-to-End Delay and Jitter are not measured during the simulation process. Moreover, MATLAB's IEEE 802.11 standard based security evaluation is not up to the mark since most of the latest IoT devices are using updated IEEE P1451.99 standard – which is the identified limitation of LEAEWSN work.

2.5. Light Weight Authentication Scheme for Smart Home IoT Devices (LWAS)

In 2022, Vipin Kumar et.al., submitted a lightweight authentication algorithm abbreviated here as LWAS [11] for the purpose of home device remote access authentication with sufficient confidentiality and authenticity. It is stated that the LWAS work provides rigid security against several security attacks such as replay attack, server spoofing, masquerade attack, offline password guessing, user impersonation and man-in-the-middle attack. Introduction of a comprehensive authentication method suitable for low power IoT devices and performance analysis of the same are the major contributions found in LWAS work. Authentication device, controlling device, user device and home appliances are getting benefit through LWAS work by simplifying the session key, private key, and public key calculations. Network Simulator NS3 is used in the experiments to measure the performance of the LWAS work. Computational overhead, communication delays and energy consumption are measured during the experiments of LWAS work.

Lower computational overhead, communication delays and energy consumption even after applying the LWAS security scheme is the noted advantage of LWAS. There is no specific relevant assessment tool used to measure the security during the experimental phase. Protection against several modern attacks are not addressed in LWAS work – which is noted as the limitation of LWAS work.

2.6. Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things (LAAKA)

Xiang Gong et.al., presented LAAKA work in 2022 to solve the power – security balance problem on IoT networks. The heterogeneous property among the IoT devices causes a power-security balance problem. That is when there is a powerful security protocol is incorporated in an IoT network environment, resource constrained battery-operated devices suffer due to high computational complexity of the security protocol. As a result, the overall network lifetime and the performance were affected significantly. While incorporating lesser computational complexity security protocols, the security of the network environment is put into vulnerability in high computational resource zones of the IoT network environment. This scenario happens since the high computational devices can easily break smaller security keys by attempting several types of attacks. Therefore, it is important to manage a perfect balance between the power and security while designing a new protocol. LAAKA work is one of the attempts to achieve the same.

LAAKA work is built over the CoAP framework. The LAAKA scheme adopts elliptic curve public key exchange mechanism and shared secret key exchange methods to ensure the anonymity for sender and receiver which improves the security and attack proof property of the communication. LAAKA method provides individual methodologies for initiation phase, registration phase, identity authentication phase, and key agreement phase.

The security analysis is performed using Colored Petri Net (CPN) tools against confidentiality, data integrity, mutual authentication, forward and backward secrecy perfection, device anonymity, device separability, impersonation attack resistance, man-in-the-middle attack resistance, Privileged insider attack resistance, known session-specific temporary information attacks resistance, replay attack resistance, key compromise impersonation attack resistance, desynchronization attack resistance, DoS attack resistance and amplification attack resistance. computational overhead and communication overhead are measured to evaluate the performance of the LAAKA work.

Achievement of lower computational and communication overhead is the observed advantage of LAAKA work whereas discontinued CPN tools-based security analysis is not up to the standard against most recent real-time IoT network attacks. Missing analysis of security using most recent simulation tool during the experiment is realized as the limitation of LAAKA work.

2.7. A lightweight three factor authentication framework for IoT based critical applications (L3FAF)

In 2022, Manasha Saqib et.al., introduced a three-factor authentication framework abbreviated here as L3FAF.The indented purpose of this work is to provide security for IoT network environments against Shadow IoT device attack without intensive computational protocols. Pattern leveraging Elliptic Curve Cryptography is used as the crypto base in L3FAF work to ensure the protect identity, password and digital signatures in an IoT network environment. L3FAF work takes care of System initialization phase, Signature generation phase, Signature verification phase, Registration phase, Login/authentication phase and Password revocation phase. Informal security analysis for confidentiality,

mutual authentication, Man-in-the-Middle attack, Replay attack, Known session key attack, Subscriber impersonation attack, Perfect forward secrecy, Broker impersonation attack, Publisher impersonation attack, Anomaly attack Trace attack, Offline password guessing attack, Privileged insider attack and Smartcard stolen attack are clearly described in L3FAF work.

The L3FAF work experiments are carried out using Scyther tool. Performance metrics such as computational cost and communication cost are measured during the experiments. One of the notable advantages of L3FAF is that, it can provide security against stolen smartcard attack which is not commonly covered in most of the security protocols. The overall processing time of the for L3FAF work is not measured during the experiments. Higher processing time due to three-factor authentication is perceived as the limitation of L3FAF work. Measurement of performance metrics such as Throughput, End-to-End delay, Packet Delivery Ratio could be beneficial to L3FAF if included as experimental parameters

2.8. Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function (LSADPUF)

In 2022, Cong Pu et.al., proposed a Physically Unclonable Function (PUF) blended with Bloom Filter for Sybil attack detection [14]. LSADPUF work is mended based on routing protocol for low powered and noise network (RPL) to target on sybil attack in RPL based IoT network environments. LSADPUF is designed to minimize the memory occupation of conventional RPL and also to reduce the attack detection latency without any impact on detection accuracy and precision. A Destination Oriented Directed Acyclic Graph (DODAG) is used to generate a bloom filter array by performing hash functions of every node's identifier and PUF response in LSADPUF work. Then DODAG is distributed to every node in the network to verify their own presence in the network and to know the identification of the other legitimate nodes. Whenever a data packet or a send request is received from a node for that there is no presence of its identification on DODAG, the received node raise a sybil attack attempt alarm to the entire network till the cluster head is aware of that. This process is taken care by the sybil Attack detection mechanism of LSADPUF work. Then the attack impact relief mechanism defined in LSADPUF will take care of the blocking of the attacker.

OmNet++ network simulator is used to evaluate the performance of the LSADPUF method during the experiments. Attack detection accuracy, detection latency, and energy consumption are measured during the LSADPUF experimental phase. Achievement of low latency, low power consumption and high detection rate of sybil attacks are the advantages of LSADPUF work whereas, security against other attacks excluding sybil attack is not addressed by LSADPUF – which is observed as the limitation of this model.

2.9. A lightweight D2D security protocol with request- forecasting for next-generation mobile networks (LDSP)

In 2022, Daniel Gerbi Duguma et.al., proposed A lightweight device-to-device communication security protocol [15] abbreviated here as LDSP. The target of LDSP work is to ensure security between the devices in particular at 5G assisted network environments. LDSP work combines specific procedures for initialization phase, Device discovery phase and link setup phases. LDSP protocol is build based on a new network function called D2D Security Management Function (DSMF) along with deep learning base UE trust score forecasting. The security of LDSP work is verified through two different methods. The first method is BAN logic and the second method is scyther tools. Different types of IoT network security factors such as lightweight cryptographic operations, anonymity, mutual authentication, confidentiality, integrity, and forward security are considered in the LDSP work. The initial assumptions required for LDSP are 5G serving network, all DSMF devices should be connected with the 5G network, Unique ID expose before running initiating the protocol and 5G global unique temporary identifier dependability for maintaining privacy and anonymity. A typical 5G D2D communication network environment is illustrated in Figure 2.

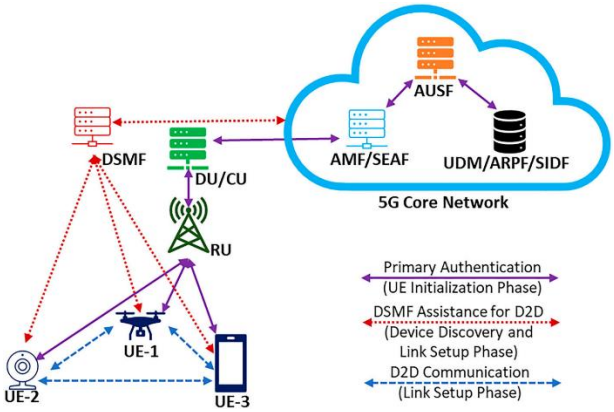

Figure 2: 5G based D2D Communication Network Model

The communication latency is calculated during the experiments. Achievement of security using lightweight cryptographic method and lower communication latency are the advantages of LDSP network. The complicated initial assumptions make the LDSP work into a vulnerable one for latest attack types. Throughput and packet delivery ratio parameters are not included in the experiment, which can be the limitation of LDSP work.

2.10. L-ECQV: Lightweight ECQV Implicit Certificates for Authentication in the Internet of Things

In 2023, Manisha Malik et.al., introduced a new lightweight version of Elliptic Curve Qu Vanstone (ECQV) certification method abbreviated as L-ECQV [16]. The main motive of L-ECQV work is to provide true end-to-end security for data in the IoT based network environments. A novel encoding mechanism is introduced in L-ECQV method which has a lightweight profile. Device authentication, secure data transfer, secure firmware updates, and remote access control strategies are clearly discussed in L-ECQV work. Parameters such as certificate sizes, handshake message overhead, certificate validation time, and energy consumption time are measured during the experiments carried out for L-ECQV work. Network entities required to apply L-ECQV work are factory server, certificate authority, IoT device, and a resource rich 6LoWPAN border router. The L-ECQV work removes some of the certificate parameters from the conventional ECQV certification model to maintain the lightweight profile.

Achievement of 27% reduction in power consumption and a 52% reduction on handshake message overhead are the observed advantage of L-ECQV work. Essential IoT network performance parameters such as throughput, end-to-end Delay, and packet delivery Ratio are not included in the evaluation process of L-ECQV, which is the noted limitation of L-ECQV work.

2.11. Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications (SLAP)

Sunil Gupta et.al., introduced a Secure and Lightweight Authentication Protocol (SLAP) [17] for improving privacy in smart city application communications. SLAP work addresses setup phase, user registration phase, sensor registration phase, login phase, user authentication / key exchange phase, password update phase, and revocation phase by introducing proper procedures. SLAP method combines the network entities such as user gateway, Private key of gateway, sensor identity, sensor public key, sensor private key, user identity, user password, one-way hash function, smart card, prime numbers, communication delays, and timestamps for the process of authentication. The informal security verification is done by using the BAN logic. The formal security verification is carried out by the AVISPA tool with High Level Protocol Specification Language (HLPSL). Security privacy resource constrains, scalability, compatibility and development / deployment Costs are discussed in SLAP work.

Achievement of lower energy consumption is the stated advantage of SLAP work. Simulation readings are not taken for most important network performance metrics such as Throughput, Communication Delays, Packet Delivery Rate, and Security level, which is the observed limitation of SLAP work.

2.12. A user-centric privacy-preserving authentication protocol for IoT-AmI environments (UCPAP)

In 2022, Mehedi Masud et.al., proposed an User Centric Privacy-preserving Authentication Protocol (abbreviated here as UCPAP) for IoT-ambient intelligence network environments. UCPAP is developed based on blockchain and fog computing technologies to ensure the unforgettability, non-repudiation, low latency, transparency, and for

effective bandwidth utilization. PUF, Biometrics and Ethereum based smart contracts to resist cloning attack, Impersonation attack and Replay attack. UCPAP is designed in a way to minimize the communication cost and resource consumption. User registration phase, IoT sensor node registration phase, mutual authentication and key agreement phase are clearly discussed in UCPAP work. Scyther tool is used to evaluate the security performance of UCPAP work.

Achievement of security wilt limited resource consumption is the advantage of UCPAP work. Hard to follow initial assumptions are understood as the limitation of UCPAP work. Assumption of tamper proof gateway me the UCPAP vulnerable to insider attacks which is also identified as another limitation of UCPAP work.

2.13. An Improved Lightweight User Authentication Scheme for the Internet of Medical Things (ILUAS)

In 2023, Keunok Kim et.al., introduced a lightweight authentication scheme for Internet-of-Medical Things (IoMT). IoMT is one of the domain specific architecture to support the medical industry in particular. ILUAS targets on security against offline password guessing attacks by incorporating biometric based authentication. The replay attack is rectified by a dedicated logic for the gateway to authenticate the user. Privileged insider attack is reduced by deleting the temporary transactional data from the memory. ILUAS is majorly constructed using hash functions and XOR operations. The system model architecture of ILUAS work is provided in Figure 3.

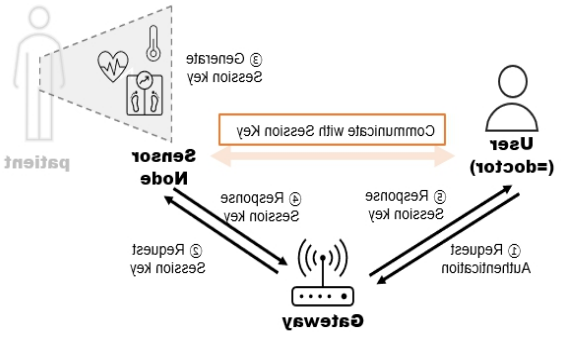

Figure 3: ILUAS system model

The complete security analysis is performed theoretically in the paper. Experiments based on real-time security measurement tools or based on simulation are not discussed in ILUAS work. The communication cost is also computed based on the formula which is lacking real-time environmental impact. Incorporation of biometric data during the authentication, lightweight hash function and XOR operations are the specialty of ILUAS work whereas absence of real-time or simulation-based performance evaluation is the limitation.

2.14. A Lightweight and Robust User Authentication Protocol with User Anonymity for IoT-Based Healthcare (LRUAP)

Chien-Ming Chen et.al. proposed a Lightweight and Robust User Authentication Protocol condensed here as LRUAP [20] to enhance user anonymity in IoT healthcare systems. User registration phase, sensor registration phase, login and mutual authentication phase, threat model, perfect forward secrecy, privilege insider attack, stolen verification attack, and sensor node capture attack are discussed elaborately in LRUAP work. The security of LRUAP work is analyzed using Real-or-Random (ROR) model. Processing time, communication cost and security parameters are taken in the comparison section. The security level is theoretically discussed with binary results. The XOR operation and non-collision hash function is the reason behind the lower communication cost.

Achievement of lower communication cost and lesser processing time are the advantage of LRUAP mode. Real or simulated environment based precise security measurement is not carried out as an experiment in LRUAP work realized as the limitation.

2.15: LMAS-SHS: A Lightweight Mutual Authentication Scheme for Smart Home Surveillance

In 2022 Saeed Ullah Jan et.al., introduced LMAS-SHS [21] work for the purpose of lightweight robust mutual authentication in IoT network meant for smart home monitoring system. LMAS-SHS is based on hash cryptographic function and elliptic curve cryptography along with XOR operations for mutual authentication function. LMAS-SHS provides individual procedures for Setup phase, Mobile Registration phase, smart object registration phase, and mutual authentication phase. The theoretical security analysis is performed in LMAS-SHS work using Gong-Needham-Yahalon (GNY) logic. The programmatic security analysis is carried out in

LMAS-SHS work using ProVerif protocol analyzing tool.

LMAS-SHS model withstands several attacks such as insider attack, traceability attack, Denial-of-Service (DoS) attack, replay attack, man-in-the-middle attack, de-synchronization attack, and stolen verifier attack. Computational cost is calculated during the experiments in which the processing time of elliptic curve cryptography exponential calculation is excluded, thus stated as the low processing time.

Achievement of anonymity is the achievement of LMAS-SHS work. Leftover performance metrics such as throughput, communication delays, packet delivery ratio and energy consumption are identified as the limitations of LMAS-SHS work.

III. EXISTING METHODS TABLE

A brief description of existing methods, methodologies used, their advantages and the limitations are tabulated and given in Table 1 comprehensively for comfortable comparison.

S. No.	Author	Year	Work	Methodologies	Advantages	Limitations
1	Jhonattan J. Barriga et.al.	2022	Securing End-Node to Gateway Communication on LoRaWAN with a lightweight security protocol	LoRaWAN Protocol enhancement	Better processing speed, Lower power consumption	Throughput, Communication delays Packet Delivery Ratio
2	Haseeb-ur-rehman RMA et.al.	2022	LR-AKAP: A Lightweight and Robust Security Protocol for Smart Home Environments	Symmetric Key based Authentication Protocol	Improved Security	Higher Computational and Communication overheads
3	A. Ahmed Introduced et.al.	2023	Light-Weight Security Protocol and Data Model for Chip-to-Chip Zero-Trus	C2CZT communication protocol enhancements	Improved Security	Higher Computational and Communication overheads
4	Ntebatseng Mahlake et.al.	2022	A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things	XOR and XNOR based key exchange mechanism	Improved Security, Higher PDR, Lower Energy consumption	Throughput, Communication delays
5	Vipin Kumar et.al.	2022	Light Weight Authentication Scheme for Smart Home IoT Devices	Authentication protocol enhancements	Lower computational and communication overheads, Lower energy consumption	Vulnerable to modern attacks

6	Xiang Gong et.al.	2022	Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things	CoAP ECC key exchange	Lower computational and communication overheads	Compromised Security
7	Mansha Saqib et.al.	2022	A lightweight three factor authentication framework for IoT based critical applications	Pattern Leveraging ECC Three-factor authentication	Security against stolen smartcard attack	Higher Processing time
8	Cong Pu et.al.	2022	Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function	Destination Oriented Directed Acyclic Graph Bloom filter	Attack detection accuracy, Low Latency, Lower Energy Consumption	Vulnerable to many attacks other than Sybil attack
9	Daniel Gerbi	2022	A lightweight D2D	D2D Security Manag	Light weight, Lower	complicated initial assum
	Duguma et.al.		security protocol with request-forecasting for next-generation mobile networks	ement Function (DSMF), Deep learning base UE trust score forecasting	communication delay	ptions increase deployment intricacy
10	Manisha Malik et.al.	2023	L-ECQV: Lightweight ECQV Implicit Certificates for Authentication in the Internet of Things	Elliptic Curve Qu Vanstone (ECQV) certification	Reduced power consumption	Increased Communication overheads
11	Sunil Gupta et.al.	2023	Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications	Authenticaton protocol enhancements	Lower Energy consumption	Increased Communication overheads
12	Mehedi Masud et.al.	2022	A user-centric privacy-preserving authentication	Blockchain, Fog computing	Moderate security with lesser resource consu	complicated initial assumptions increase deploy

			protocol for IoT-AmI environments		mption	ment intricacy
13	Keunok Kim et.al.	2023	An Improved Lightweight User Authentication Scheme for the Internet of Medical Things	Hash functions and XOR operations	Biometric data, Lightweight Hash functions	Vulnerable to modern attacks
14	Chien-Ming Chen et.al	2021	A Lightweight and Robust User Authentication Protocol with User Anonymity for IoT-Based Healthcare	Non-collision Hash functions	Lower communication cost and processing time	Vulnerable to modern attacks
15	Saeed Ullah Jan et.al.	2022	LMAS-SHS: A Lightweight Mutual Authentication Scheme for Smart Home Surveillance	Hash cryptographic function and Elliptic Curve Cryptography	Higher Anonymity protection	Increased computational and communication overheads

Table 1: Existing methods comprehensive summary

IV. CONCLUSION AND SCOPE FOR NEW RESEARCH WORKS

Based on the gathered data and studies of the existing works, it is understood that there are three primary considerations discovered for the progressions of IoT based Services. They are security, power consumption and network Performance. Initially, the innovations towards IoT network service improvement works are developed to improve any of the above-mentioned factors those affect the remaining factors negatively [22]. Thus, the recent research works concentrates on more than one constrains such as power-security balanced, or security-performance balanced or performance-power balanced. Most of these works provides improvement in one factor without affecting the another considered factor. There are very few works those support improvements in both considered factors where one of the factor's improvement is not significant.

Therefore, it is identified that there is a huge scope for the multi-constrained improvement or optimization model-based research works are necessary to improve generic IoT based network services.

Conflict of Interest: The authors declare there is no conflict of interest

Funding: This survey is carried out for individual research work, thus external funding is not inclined

Data Availability Statement: All data are collected from reputed public domains available online

REFERENCES

[1] Sree Krishna Das, Fatma Benkhelifa, Yao Sun, Hanaa Abumarshoud, Qammer H. Abbasi, Muhammad Ali Imran, Lina Mohjazi, "Comprehensive review on ML-based RIS-enhanced IoT systems: basics, research progress and future challenges," in Computer Networks, Volume 224, 2023, 109581, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2023.109581

[2] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller, "Landscape of IoT security," in Computer Science Review, Volume 44, 2022, 100467, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2022.100467

[3] Gunjan Beniwal, Anita Singhrova, "A systematic literature review on IoT gateways", in Journal of King Saud University - Computer and Information

Sciences, Volume 34, Issue 10, Part B, 2022, Pages 9541-9563, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2021.11.007

[4] Arshad, QuA., Khan, W.Z., Azam, F. et al. Blockchain-based decentralized trust management in IoT: systems, requirements and challenges. Complex Intell. Syst. (2023). https://doi.org/10.1007/s40747-023-01058-8

[5] S. Das and S. Namasudra, "Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 821-829, Jan. 2023, https://doi:org/10.1109/TII.2022.3167842

[6] Yakub Kayode Saheed, Aremu Idris Abiodun, Sanjay Misra, Monica Kristiansen Holone, Ricardo Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things" in network attacks, Alexandria Engineering Journal, Volume 61, Issue 12, 2022, Pages 9395-9409, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2022.02.063

[7] J. J. Barriga and S. G. Yoo, "Securing End-Node to Gateway Communication in LoRaWAN With a Lightweight Security Protocol," in IEEE Access, vol. 10, pp. 96672-96694, 2022, https://doi:org/10.1109/ACCESS.2022.3204005

[8] Haseeb-ur-rehman RMA, Liaqat M, Aman AHM, Almazroi AA, Hasan MK, Ali Z, Ali RL. LR-AKAP: A Lightweight and Robust Security Protocol for Smart Home Environments. Sensors. 2022; 22(18):6902. https://doi.org/10.3390/s22186902

[9] A. Ahmed, A. Shoufan and K. Belwafi, "Light-Weight Security Protocol and Data Model for Chip-to-Chip Zero-Trust," in IEEE Access, vol. 11, pp. 60335-60348, 2023, https://doi:org/10.1109/ACCESS.2023.3285630

[10] Mahlake, Ntebatseng, Topside E. Mathonsi, Deon Du Plessis, and Tonderai Muchenje. "A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things." J. Commun 18 (2023): 47-57.

[11] Kumar V, Malik N, Singla J, Jhanjhi NZ, Amsaad F, Razaque A. Light Weight Authentication Scheme for Smart Home IoT Devices. Cryptography. 2022; 6(3):37. https://doi.org/10.3390/cryptography6030037

[12] Gong X, Feng T. Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things. Sensors. 2022; 22(19):7191. https://doi.org/10.3390/s22197191

[13] Manasha Saqib, Bhat Jasra, Ayaz Hassan Moon, "A lightweight three factor authentication framework for IoT based critical applications," in Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, 2022, Pages 6925-6937, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2021.07.023

[14] Cong Pu, Kim-Kwang Raymond Choo, "Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function," in omputers & Security, Volume 113, 2022, 102541, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102541

[15] Daniel Gerbi Duguma, Jiyoon Kim, Sangmin Lee, Nam-Su Jho, Vishal Sharma & Ilsun You, "A lightweight D2D security protocol with request-forecasting for next-generation mobile networks," in Connection Science, 34:1, 362-386, https://doi.org/10.1080/09540091.2021.2002812

[16] M. Malik, Kamaldeep, M. Dutta and J. Granjal, "L-ECQV: Lightweight ECQV Implicit Certificates for Authentication in the Internet of Things," in IEEE Access, vol. 11, pp. 35517-35540, 2023, https://doi.org/10.1109/ACCESS.2023.3261666

[17] Gupta S, Alharbi F, Alshahrani R, Kumar Arya P, Vyas S, Elkamchouchi DH, Soufiene BO. Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications. Sustainability. 2023; 15(6):5346. https://doi.org/10.3390/su15065346

[18] Mehedi Masud, Gurjot Singh Gaba, Pardeep Kumar, Andrei Gurtov, "A user-centric privacy-preserving authentication protocol for IoT-AmI environments," in Computer Communications, Volume 196, 2022, Pages 45-54, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2022.09.021

[19] Kim, Keunok, Jihyeon Ryu, Youngsook Lee, and Dongho Won. 2023. "An Improved Lightweight User Authentication Scheme for the Internet of Medical Things" Sensors 23, no. 3: 1122. https://doi.org/10.3390/s23031122

[20] Chien-Ming Chen1, Shuangshuang Liu1, Shehzad Ashraf Chaudhry, Yeh-Cheng Chen3 and Muhammad Asghar khan, "A Lightweight and Robust User Authentication Protocol with User Anonymity for IoT-Based Healthcare," in Computer Modeling in Engineering & Sciences, Tech Science Press, 2021, http://dx.doi.org/10.32604/cmes.2022.018749

[21] S. U. Jan, I. A. Abbasi and M. A. Alqarni, "LMAS-SHS: A Lightweight Mutual Authentication Scheme for Smart Home Surveillance," in IEEE Access, vol. 10, pp. 52791-52803, 2022, https://doi:org/10.1109/ACCESS.2022.3174558

[22] Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, Ioanna Kantzavelou, "IoT: Communication protocols and security threats," in Internet of Things and Cyber-Physical, Systems, Volume 3, 2023, Pages 1-13, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2022.12.003