IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received February 9, 2022, accepted March 7, 2022, date of publication March 16, 2022, date of current version April 6, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3160000

Types of Lightweight Cryptographies in Current Developments for Resource Constrained Machine Type Communication Devices: Challenges and Opportunities

SHAFI ULLAH[1,2], RAJA ZAHILAH RADZI[1], (Member, IEEE), TULHA MOAIZ YAZDANI[3], ALI ALSHEHRI[4], AND ILYAS KHAN[5]

[1]School of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia
[2]Department of Computer Engineering, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta 87300, Pakistan
[3]Department of Electrical Engineering, College of Engineering, Majmaah University, Al-Majmaah 11952, Saudi Arabia
[4]Department of Computer Science, University of Tabuk, Tabuk 47512, Saudi Arabia
[5]Department of Mathematics, College of Science Al-Zulfi, Majmaah University, Al-Majmaah 11952, Saudi Arabia

Corresponding authors: Tulha Moaiz Yazdani (t.kamran@mu.edu.sa) and Ilyas Khan (i.said@mu.edu.sa)

This work was supported in part by the U.S. Department of Commerce under Grant BS123456. The work of Tulha Moaiz Yazdani was supported by the Deanship of Scientific Research at Majmaah University under Project R-2022-84.

ABSTRACT Machine-type communication devices have become a vital part of the autonomous industrial internet of things and industry 4.0. These autonomous resource-constrained devices share sensitive data, and are primarily acquired for automation and to operate consistently in remote environments under severe conditions. The requirements to secure the sensitive data shared between these devices consist of a resilient encryption technique with affordable operational costs. Consequently, devices, data, and networks are made secure by adopting a lightweight cryptosystem that should achieve robust security with sufficient computational and communication costs and counter modern security threats. This paper offers in-depth studies on different types and techniques of hardware and software-based lightweight cryptographies for machine-type communication devices in machine-to-machine communication networks.

INDEX TERMS Attribute based encryption, elliptic curve cryptography, identity based encryption, Internet of Things, lightweight cryptography, machine type communication devices, machine-to-machine communication, signcryption.

I. INTRODUCTION

Machine type communication (MTC) devices have recently evolved to proclaim industry 4.0. The devices used, are fully automated that support smart factory, smart workshop, smart healthcare and surveillance systems, working endlessly, generating data and making policy based decisions, used all over the world for certain smart and automation purposes and the demand is expected to increase to 50 billion by 2025 [26].

These devices require the same sort of security as other computing devices have. In some cases, even more because of the extreme vulnerability and usage in open environments. The best way researchers adopted to provide the demanded security, is through lightweight cryptography since MTC devices cannot afford adoption of heavy cryptosystems due to small computational and memory capabilities. Consequently, lightweight cryptographic schemes are proposed for data, devices, and networks so that strong encryption can be afforded to improve security [33], [37]–[42]. There is huge demand for reliant and cost-effective lightweight cryptography, adoptable by such resource constrained devices in constrained environments. It is highly efficient to improve cryptographic security provisions in growing number of resource constrained IoT devices rather than replacing all devices with powerful computational capabilities.

Such MTC devices are autonomous whose sole purpose is to automate the entire framework of IoT. The devices and its' operations have evolved from IoT to support the concept of industrial revolution 4.0. It can address to same applications of IoT by offering more advancement in operations,

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

automation, and adaptability. A system of such devices makes M2M communication network where large number of resource-constrained independent devices makes an autonomous system. These are also named as cyber-physical systems and edge nodes [57].

This paper represents an in-depth study that is primarily based on perception layer developments through lightweight cryptographic approaches used in MTC devices that serves different IoT applications, cyber-physical systems (CPS) and M2M communication networks. These applications are characterized based on the type of solutions proposed for systems in terms of applied cryptosystems, security analysis, performance measurements and environmental factors. Then, a comparative study is made on the lightweight solutions offered by the schemes for resource constrained devices.

A. RESEARCH CONTRIBUTION

This work introduces an extensive idea on research applied on different types of lightweight cryptographic techniques in perception layer of resource constrained M2M communication and IoT networks. The work further offers an overview of strengths, weaknesses issues and challenges in several research articles on lightweight cryptographies and suggests expandable solutions, recommends research gaps, and highlights future directions (in section 3). The taxonomy further offers a brief insight on recent lightweight developments in resource constrained MTC and IoT devices.

B. PAPER STRUCTURE

The lightweight cryptographic types are briefly discussed in section 2 and each subsection is presented with a summarized table. At the end of section 2, a comparative analysis on all mentioned types is presented along with a taxonomy. Section 3 describes the issues and challenges found in the mention techniques and offer a future direction on devising a lightweight technique whereas the conclusion is discussed at the end.

II. LIGHTWEIGHT CRYPTOGRAPHY

Primitive cryptographic techniques are modified to be cost effective in memory and computation in delivering robust security, is called lightweight cryptography [62]. Development of lightweight techniques consider analyzing the demands on hardware, computational complexity, memory consumptions and limitations of the IoT devices and M2M networks [5]. Lightweight cryptography is mainly adopted due to low computational capability and lack of internal memory in devices as the techniques do not accommodate standard encryption primitives. However, it also faces many challenges [66]. To address these issues and get satisfactory security assurance in M2M communication networks, various authentication and data integrity tactics have been suggested that mainly depend on the efficacy of the lightweight cryptography in the security of IoT implementation model [67].

The lightweight cryptography must retain certain security features to be able to provide robust security to the resource constrained devices in M2M network. Since M2M communication mainly depend on perception layer communication thus it must address to basic security features of perception layer such as data integrity, data confidentiality, device authentication, and data availability, (briefly described in [69]). Some advance autonomous devices such as MTC, CPS and IIoT also work in more advanced and large networks such as health monitoring systems, autonomous industrial workshops, and sensitive data sensing and monitoring systems thus the lightweight cryptography in those networks must exhibit resilience against several modern security attacks such as Man-in-the-middle (MITM), data Spoofing, Man-at-the-End (MATE), forgery, device replication, DoS and physical attacks (briefly described in [71]). Additionally, the lightweight cryptography must also address vital security features such as collusion-resistance: an attacker that holds numerous keys can possibly have the option to get to information if any single key grants accessibility to network, forward secrecy: assures that encrypted keys cannot be compromised in keeping long-term secrets despite addition of more devices and users and backward secrecy: assures that the adversary who knows subset of keys, cannot discover the previous keys despite the addition and removal of new and old devices. In case of cloud, gateway and central devices, firewall security is also required so that unwanted access requests are denied. Moreover, the cryptographic technique is also liable to deliver secure communication with efficient power, computation, and transmission costs (described briefly in [70]).

Additionally, there have been several lightweight cryptographic innovations to improve security and deliver affordable performance. These innovations target particular hardware for specific M2M, CPS and IoT applications [72] such as TEA and Signcryption in smaller IoT, ECC for large M2M and IoT networks, ABE and IBC based lightweight cryptography for particular hardware and closed IoT network which are briefly explain the following sections.

A. ATTRIBUTE BASED ENCRYPTION (ABE)

The idea of attribute-based encryption was first proposed in 2004 [73] and later enhanced by Goyal et al. [74]. it is an asymmetric public key cryptography where the secrecy of the key is devised from the attributes of user and cipher-text with access control. In such a framework, the decryption process of a cipher-text is conceivable when the arrangement of attributes of the user key matches the attributes of the cipher-text. Vital security measures of attribute-based encryption are collusion-resistance, forward secrecy and backward. Moreover, there are two sorts of ABE plans: key-policy-ABE and cipher-text-policy-ABE. In KP-ABE, user's secrecy of the key is dependent on an entrance tree that characterizes the attributes of the concerned user whereas data is ciphered over several random and (in some cases) determined attributes. Similarly, CP-ABE utilizes access trees to scramble data and user's secret key is produced from set of attributes. CP-ABE is progressed similarly since it produces set of known attributes as Key-Policy-ABE (KP-ABE) or as systems portrayed over several attributes as devices that hold keys for same characteristics can unscramble the cipher-text. Several lightweight approaches adopted ABE cryptography due to attributes driven lightweight hash functions where the hash functions mainly encrypt the entire data block through combination of certain attributes thus removing the need to acquire computational exhaustive models to achieve high level of randomness in generating ciphers and keys.

1) ABE PRIMITIVE RESEARCH

Cooperative cipher-text (C-CP-ABE) approach is taken for the attributes dependent encryption to ensure safe data exchange through transferring the task from busy devices to unconstrained devices by means of hand-over. CPU exhausting tasks of CP-ABE encryption are transferred to the unconstrained neighbor devices. Furthermore, a busy device can also transfer substantial and expending tasks to unconstrained neighbor devices. The primary explanation for C-CP-ABE is to allocate calculation of CP-ABE encryption to neighbor devices with fewer loads. Prasetyo *et al.* [12] exhibited a blowfish computation applied on an FPGA device. Allocation of calculation to FPGA is cost effective in terms of time and computation. It diminished encryption time, produced critical throughput, and did not influence avalanche effect. In [25], author proposed CP-ABE and key management arrangement that excluded suspension of assignments, ensuring reusability of data. The system rejected computational overhead by re-encryption and renaming memory locations which devoured less memory. Yao *et al.* [44] proposed a lightweight no-matching ABE method using elliptic curve cryptography. The technique depended on ECDDH instead of bilinear Diffie-Hellman, which decreased handling and data transmission overheads. Nevertheless, ABE procedure obliges a single substantial application and cannot be deliver to pervasive M2M communication network-based applications. Authors in [55] proposed an ECC in Spartan3E (FPGA) by embedding Elgamal hash function for inspection. The exploration constrained FPGA devices brought about other ECC based encryptions in utilizing less memory and computation. Touati [58] utilized Batch-Based CP-ABE algorithm with quality revocations and introduced another strategy to diminish complexity and overhead by utilizing time-slots without requiring extra nodes. The time is separated into pieces of a comparative length called timeslots (in milliseconds) and access changes happen between two runtime timeslots. Besides, the proposed strategy require synchronization between all functional devices within the network. Touati [7] proposed KP-ABE strategy that used computational expense and memory limit of cloud servers during the authenticated of devices for data transmission. Oualha [10] proposed CP-ABE technique by using practical pre-calculation frameworks. The crucial idea was driving pre-calculation methodologies, is to store cache of set pairs with high cryptographic calculations. In addition, such pre-calculation frameworks were reliant on the generator functions that decreased the cost of CP-ABE encryption and used less calculation than the original scheme. In [18], authors displayed investigation of lightweight asymmetric encryption known as AAβ (AA-Beta) that obtained an exponential upgrade in computational expense during encryption and decryption of large 2048-bit prime numbers. In [65], Authors proposed the outsider (third party) based multi-key exchange technique and utilized ECC based cryptosystem. The strategy demonstrated security against five attacks i.e. replay, eavesdropper, disguised-node impersonation, and forgery attack. [68] presented constant size ciphertexts and secret keys (CSCTSK) scheme, favoring constant size ciphertexts and keys through AND-gate framework. The scheme successfully countered chosen ciphertext attacks. [70] presented a pairing-free access control scheme (PF-CPABE) by utilizing scalar multiplication on elliptic curves instead of bilinear-pairing. It resulted in reducing users overhead through directly revokable key distribution by system. Additionally, Table 1 provides summary of ABE based lightweight techniques in terms of achievements and weaknesses. It is notable that the mentioned techniques were primarily adopted to improve computational costs. However, there is less stress on security provisions to counter modern attacks on CPS and MTC devices.

B. IDENTITY-BASED CRYPTOGRAPHY (IBC)

Identity-based cryptography (IBC) also known as identity-based encryption (IBE), is a vital primitive of identity centered cryptography. It is a public key cryptography (PKC) where user's public key is constructed based on some unique information about user's identity. It implies that a sender, who has been granted access to the public network, can cipher a text using the text-value of the receiver's identity information as a key. The receiver attains the deciphering key pattern from a central authority (server) that is trusted as it produces secret keys for each user. The center authority can be a central database or a public key generator (PKG). Many lightweight schemes adopted such cryptographic technique as most computational exhaustive encryption tasks are handled over to a powerful central authority for execution.

1) IBC BASED RESEARCH IN LIGHTWEIGHT CRYPTOGRAPHY

IBC was initiation of identity-based cryptography which relied on signatures that remained a problematic area for years. The pairing-based Boneh–Franklin scheme [3] and Cocks' encryption scheme [11] depended on quadratic residues, both tackled the IBE issues. Identity based frameworks enable every party of produced public keys from a standard identity value such as an ASCII string. In broadcast encryption [75], the amount of content could be shared and unscrambled by numerous receivers. However, An effective broadcast encryption scheme that has a short amount of content and a short private key with high collusion resistance, was presented by Boneh *et al.* Additionally, identity based broadcast encryption was presented independently by Delerablée [76] and Sakai and Furukawa [77]. Gentry and Waters [21] presented the first adaptively secure Identity-based broadcast encryption (IBBE) scheme where a

TABLE 1. Summary of the mentioned ABE based lightweight techniques.

Articles	Techniques	Fs	CF	BSF	Achievements	Weaknesses
[5]	Cooperative hand over of computation	N	N	Y	Feasible and efficient basic security adoption	Trusted unconstrained neighbor devices
[12]	BLOWFISH Implementation on FPGA	N	Y	N	Reduce total encryption time	Costly operational hardware required.
[25]	CP-ABE based effective key organization	Y	N	N	Reduced space complexity and network overheads	Required extra authenticated nodes
[44]	No-pairing ABE Based lightweight ECC	Y	N	N	Reduced overall communication overhead	Not pertinent to ubiquitous M2M applications
[55]	FPGA-based KP-ABE Lightweight ECC	Y	Y	N	Less memory and computing cost with good security	Expensive dedicated hardware is required
[58]	Group based Batch for CP-ABE	Y	Y	N	Policy access based group encryption	Synchronization issues
[7]	KP-ABE and remote allocation of computation	Y	N	N	Heavy encryption process shifted to unconstrained nodes and a cloud server	Resource constrained trust issues with unconstrained neighbor devices
[10]	Pre-computation techniques using ECC	N	Y	N	Discarded scalar point Multiplications consume less energy	Large memory, preset calculation does not dynamically change
[64]	Fuzzy logic and identity-based encryption	Y	Y	N	Secured and function scheme without random number requirements	Large key sizes produce computational overhead
[65]	Multi-Key exchange protocol using ECC	N	Y	Y	Mutual Authentication	Computational and memory overhead
[18]	Lightweight AAβ Encryption	N	Y	Y	Improved encryption and decryption time for 2048-bit primes	Heavy computational keys with minimal security provisions
[68]	AND-gate access control	N	Y	Y	Countered chosen ciphertext attacks efficiently	Limited security in constant key sizes
[70]	Bilinear-pairing free access control	Y	Y	N	Improved computational costs	User's key invocation is control by the system

^{FS}: Forward Secrecy, ^{CF}: Collision Free, ^{BSF}: Basic security features (perception layer), ^{Y}: Yes., ^{N}: No

semi-static secure scheme adopted fixed ciphered-texts and private keys size. In a recent progression, Kim *et al.* [20] improved the proficiency of IBBE scheme by evacuating tags and streamlining the security verification. Additionally, IBBE schemes were developed to help further develop usefulness of anonymity in identity-based broadcast encryption with revocation (AIBBER), a novel cryptographic concept known for cloud servers to revoke users' identities without decryption and to achieve full anonymity in complex functions such as ABE [19]. It was first introduced by [74] that had no user anonymity. The out-sourced unscrambling [61] improved the productivity of a general framework by utilizing an outsider decoding computations without uncovering the mystery. After a fundamental presentation from Green at al [78], outsourced unscrambling is effectively researched for public key encryption for attribute-based encryption. Additionally, Table 2 summaries the overall adoption purposes of IBC schemes, mentioned in this section. It can be elaborated that the IBC schemes mainly targeted user anonymity by involving several attributes of user and to balance the computational overheads, third-party's computational capabilities were used. However, third-party association in secure networks is still a challenging issue as it is a demanding target for adversaries.

C. ELLIPTIC CURVE BASED LIGHTWEIGHT CRYPTOGRAPHY (ECC)

Elliptic curve cryptography is one of the most famous type of lightweight and strong cryptographies used in IoT networks due to less memory consumption. ECC in a Gaussian field G, is a one-way function as its' inverse is incomputable. An elliptic curve having a field $Fp\,(a,b)\,|p > 3$ and a prime number. P represents a set of points $p(x,y)$ where $(x, yEFp(a,b))$ that satisfies equation $y^2 = x^3ax + b$ mod (p) for $0 <= x <= p$. The ECC security strength depends on computing a scaler or fixed-point multiplication as size of the curve governs the computational costs. Moreover, ANSI X9.63 and IEEE P1363 provides the PKC standard for ECC based cryptography. These standards offer randomness and security per-bit compared to the recent PKC such as RSA and AES. The applications of ECC are found in several resource constrained IoT environments where autonomous devices are deployed. There are two main arithmetic operations involved: point addition and point double during

TABLE 2. Summary of mentioned IBC based lightweight techniques.

Article	Technique	Feature	Fs	CF	BSF	Achievement	Weakness
[3]	Cocks' encryption scheme	Certificate based encryption	N	N	Y	Tackled the IBE issues	Produces Too many public keys
[11]	Fog computing security	User and device authorization-based security	Y	Y	N	Private and dynamic keys-based identities	Fog computing based secure identity issues
[35]	GBAAM-AKA	Certificate based identity	Y	N	Y	Group based identity certificates	High computational overheads
[19]	Broad Cast encryption with user anonymity	AIBBER	Y	Y	N	Efficient Resource usage of user's identities	User anonymity in cloud
[20]	Semi-static security verification	IBBE	Y	N	Y	Streamline security verification	Lack of user anonymity
[21]	Semi-static secure	IBBE	N	Y	N	Security verification	Security verification issues
[61]	User security in public cloud servers	Outsider decoding computations	Y	N	Y	ABE utilized Increased Productivity	Third-party security is weak
[63]	Lightweight mutual authentication	Efficient Key distribution	N	Y	Y	Affordable communication costs	Weak analysis of threat model

^{FS}: Forward Secrecy, ^{CF}: Collision Free, ^{BSF}: Basic security features (perception layer), ^{Y}: Yes., ^{N}: No

multiplication. Point addition refers to the addition of two points on curve. In many techniques the double-and-add algorithm or one of its variants are used to create random pattern of points on curve. Furthermore, Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Diffie-Hellman (ECDDH), Elliptic Curve Discrete Logarithm Problem (ECDLP), Elliptic Curve Integrated Encryption Scheme (ECIES), Elliptic Curve Digital Signature Algorithm (ECDSA), Edwards-curve Digital Signature Algorithm (EdDSA), Elliptic Curve Menezes-Qu-Vanstone (ECMQV) are famous flavors of ECC, as shown in Figure 1. Similarly, there are several types of curves used for different types of security provisions and curve performances. M-221, E-222, NISTP-224, Curve1174, Curve25519, BN (2,254), brainpoolP256t1, ANSSI FRP256v1, NIST P-256, secp256k1, E-382, M-383, Curve383187, brainpoolP384t1, NIST P-384, Curve41417, Ed448-Goldilocks, M-511 and E-521 are some of the famous curves used. The ECC is adopted in numerous lightweight schemes due to robust keys with minimum size. Private or public keys used in traditional encryption techniques such as RSA, AES and Elgamal are of heavy sizes. On the contrary, the ECC based keys generation is comparatively very affordable that offers the same level of key strength required in heavy encryption and decryption processes.

1) ELLIPTIC CURVE BASED LIGHTWEIGHT CRYPTOGRAPHY IN RESOURCE CONSTRAINED IoT DEVICES

Though there have been numerous developments in ECC, this article covered the schemes that targeted resource constrained devices in constrained M2M networks. [14] Implemented ECDH key exchange applying one fixed-basepoint and one variable point scalar multiplication on AVR ATmega, MSP430X and ARM Cortex M0 microcontrollers using curve25519. The curve25519 supports 255-bit curve bandwidth whereas the previous standard curves (NIST P-256 and NIST K233) supported 128-bit only. The difference in

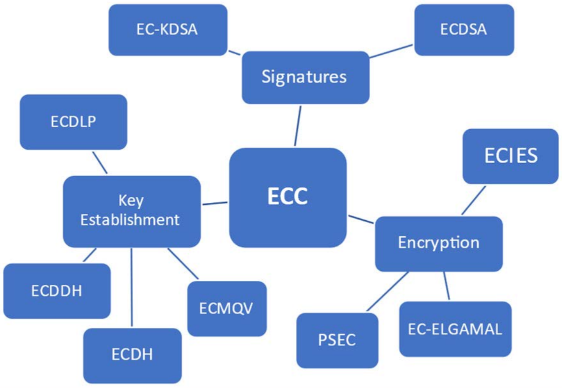

FIGURE 1. Lightweight elliptic curve cryptographic curve classification.

curve bandwidth improves the robustness of curve25519 and the cost of cycles by 18%. Previous works [24], [79]–[85] used same microcontrollers with mixed adoption of curves. The computational cost analysis is based on the type of curve and microcontroller they used. The clock cycles consumed, indicate that these resource constrained computing capable microcontrollers handled encryption computational tasks in affordable time and memory. However, the previous works avoided undisclosed data-dependent branches as well as secretly indexed the memory access to safeguard against timing attacks but could not fully counter side channel and horizontal attacks. [56] also implemented curve25519 targeted for ARM Cortex-M4 microcontroller using ECC based a digital signature (qDSA). [27] proposed mutual authentication scheme between a user, device and a gateway. [29] worked on devising a sophisticated IoT framework for achieving optimum security in a three-layer architecture with ECC based cryptographic key generation on random time points using ECG of the patients by calculating values of two crusts with the combination of Fibonacci linear feedback shift register for purpose of generating keys.

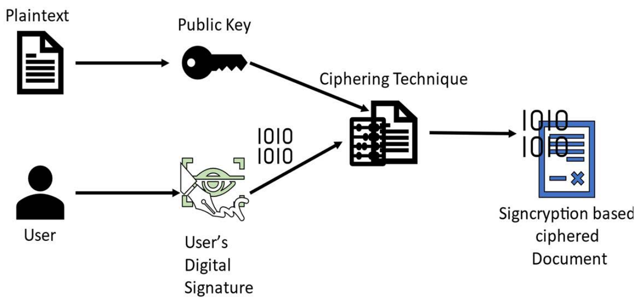

FIGURE 2. Signcryption ciphering process.

Several implementations of ECC used AVR Atmega aiming at low security levels (80-96 bits). Whereas TinyECC library applied ECDSA, ECDH, and ECIES on 128, 160 and 192-bit respectively, using SECG curves [86]. Nano ECC used the NIST K-163 curve [87]. In addition, recent ECC applications in AVR Atmega applied comparatively low-level security curves. Liu *et al.* [48] stated a novel milestones for ECC on NIST P-192 curve for speedy calculations. Similarly, twisted Edwards curves presented in [28], applied 80-bit and 96-bit security levels for performance enhanced implementation of ECC. Additionally, Table 3 provides summery of the mentioned ECC schemes in this section. Variety of schemes cover many aspects of ECC functionality. It can be elaborated that ECC has advanced in the scope and ability, to achieve a comprehensive lightweight cryptographic scheme that can counter extreme modern attacks.

D. SIGNCRYPTION

It is a PKI based lightweight cryptographic primitive concurrently perform the functions of both digital signature and encryption which are two central cryptographic tools that can assure achievement of confidentiality, integrity, and non-repudiation using less computational and communication power thus it is considered a lightweight encryption technique [17]. Signcryption based novel cryptographic technique satisfies the functionalities of digital signature and encryption in a singular logical step. In customary public key cryptography, the document is first digitally signed then encrypted the signed document for transmission over a public network. Moreover, signature-then-encryption accomplishes the procedure of the two, data encryption and authentication. However, it has two disadvantages of less efficiency and expensive computation as it diminishes computational expense when contrasted with signature-then-encryption scheme. Moreover, it contains two essential security properties (Integrity and confidentiality) in any signcryption scheme. Forward secrecy and public key verification are additional features that are adopted by signcryption relying on the necessities.

1) PRIMITIVE RESEARCH ON SIGNCRYPTION SCHEMES

Authors in [88], introduced several signcryption schemes where each design had its own advantages and downsides. Whereas, in recent developments, authors in [17] presented a techniques equipped wih indistinguishability and unforgeability to counter adaptive chosen cipher text attacks against a possible adaptive massage access code (MAC) attack under hyperelliptic curve decisional Diffie Hellman (HEDHP) and hyperelliptic curve discrete logarithm (HECDLP) problem which is implemented in the random oracle model (ROM). Similarly, authors in [52] offered an efficient cloud driven secure data sharing scheme. The scheme is supervised by an administrator who transfers all rights of signcryption to a proxy-agents where the agent generated signcryption based encrypted data on the behalf of the administrator. The proxy agent then uploads that encrypted data to the cloud server where authorized users can download and decrypt it. Guo and Deng [59] presented an efficient lightweight scheme in terms of computation cost. Both schemes use ECC based private key generation for secure signatures. The devices with limited computational resources handled lightweight encryption process at the cloud server. Horng *et al.* [30] proposed a productive endorsement less collective signature scheme for vehicular sensor networks (VSN). The proposed scheme accomplished the contingent privacy preservation and security against existential forgery on adaptively chosen plaintext attacks. F. Li *et al.* [60] recommended a heterogeneous ring signcryption technique for secure network. The encryption is between a busy device and a server over the public network. The work exhibited in [32], [89], [90], referred to firewall for ongoing authentication protocols and their applications, is a security system that screens the network traffic that depended on certain policies. However, only a few schemes are appropriate for firewalls due to disadvantages and restrictions in every scheme. [32] Proposed lightweight scheme for authentication of two-hop central wireless body area network (WBAN) that provided unidentified and unlink-able variables to wearable sensor devices and achieved mutual authentication between wearable sensors devices and end-nodes. Additionally, the scheme executed hash and XOR operations only. Iqbal *et al.* Furthermore, [34] presented another productive signcryption scheme based on elliptic curve for firewalls guaranteeing that the scheme is secure and none can copy the message access code (MAC). In recent years, [33] analysis showed that the plan proposed in [34] was not verified and had numerous security defects. The work presented the signcryption scheme introduced by [33] improved the work of [34] by achieving more basic security features and improved the scheme by using EDLP based certificate in asymmetric cryptosystem. Additionally, Table 4 summaries features in signcryption scheme mentioned in this section. It can be said that the signcryption based schemes still try to improve computational cost to secure signatures. There are variety of adopted to deliver optimal solution to avoid signature vulnerability in signcryption.

E. TEA (TINY ENCRYPTION ALGORITHM)

TEA is one of the most effective lightweight techniques in connected devices in M2M and IoT networks in contrast to other lightweight encryption techniques. A portion of the

TABLE 3. Summary of mentioned ECC based lightweight techniques.

Article	Protocol	Curve Type	Implementation	Achievement	Weakness
[4]	ECDSA_P256	SECG Curves	MQTT in Transport Layer	High security levels (256bits)	Requires internet, ineffective for MTCDs
[14]	ECDH	Curve25519	AVR ATmega, MSP430X ARM Cortex M0	Robustness Cost effective	Consume double computation due to heavy curve
[24]	ECDLP	Mixed adoption of curves	MSP430X ARM Cortex	Small scale device afforded computation	Side channel attacks horizontal attacks
[48]	ECDSA, ECDH	NIST P-192	AVR ATmega	Small scale device afforded computation	Effective only for small MTCDs
[56]	ECqDSA	Curve25519	ARM Cortex-M4	Up to 50% optimized Operations	Inefficient implementation technique
[27]	ECDH	NIST P-256	3GPP Network	Low computational and memory requirements	Database related threats and optimization
[29]	ECDDH	ECG based IPI-PRNG	Wireless Local Network	Robust random curve points	Secure authorization and effective authentication of all devices

^{MQTT} Message queuing telemetry transport

TABLE 4. Summary of mentioned signcryption based lightwieght techniques.

Article	Signature	Cryptosystem	FS	FiS	PV	Achievement	Weakness
[8]	Private, public keys by Key generator	Asymmetric encryption	Y	N	Y	Encryption and authentication	Generated keys' strength is ignored
[17]	Proxy Key Generation	Hyper ECC based asymmetric encryption	N	Y	Y	Signature dynamic key size decreased	expensive HCC Bilinear pairing
[30]	Private key based collective signatures	Symmetric encryption	Y	N	Y	Forgery attacks are countered	Expensive Symmetric encryption
[52]	Identity-based proxy Signature	ECDH based asymmetric cryptosystem	Y	Y	N	Robust large keys generated via cloud	Generated heavy proxy keys for IIOT devices
[34]	Dynamic private keys	ECC based asymmetric cryptosystem	Y	Y	N	Affordable computation	Security flaws
[59]	Polynomial time algorithm based private key signatures	DDH based asymmetric cryptosystem	Y	N	Y	Non bilinear driven lightweight key generation	Extremely high computational cost of pairing operation
[60]	Ring signcryption	Asymmetric cryptosystem	Y	N	Y	Confidential authentication	Bilinear pairings cost heavy computation
[32]	Identity based keys	Asymmetric encryption	N	Y	N	Efficient mutual authentication	Weak third-party security
[33]	Private keys' certificates	ECC based asymmetric cryptosystem	Y	Y	Y	Achieved MATE security	Neglected certificate performance

^{FS}: Forward Secrecy, ^{FiS}: Firewall Security, ^{PV}: Public Verification, ^{Y}: Yes., ^{N}: No

fascinating highlights of TEA is the simplicity of usage, non-appearance of specific standards, great execution and short enough to incorporate into any machine type communication (MTC) device. The principle focal point of TEA is to minimize memory utilization and expand speed.

1) TEA IMPLEMENTATION IN IoT

Abdelhalim *et al.* [9] proposed the Modified version of TEA (MTEA), which increased the security and power utilization. The linear feedback shift register (LFSR) is operated in a pseudo-random number generator to increase the security of the TEA and decrease energy consumption. Zhdanov and Sokolov proposed an algorithm [15] depending on the standards of many esteemed logic and variable block length techniques. The encryption procedure was performed iteratively in five sequences. Furthermore, lightweight encryption algorithm (LEA) is a block encryption algorithm [23] that was intended to offer confidentiality in lightweight condition in cell phones. Abdullah *et al.* [45] proposed a super-encryption cryptography with word auto key encryption (WAKE) calculation and international data encryption algorithm (IDEA).The DES algorithm did not permit adaptability in Feistel structure and henceforth did not bolster any adjustments in it, as discussed in [37]. Dian Rachmawati *et al.* [38] proposed an algorithm that used a joined asymmetric and symmetric encryption for secure record move. The security of the document was adopted in consideration by the symmetric algorithm "TEA" and security of the key by the asymmetric algorithm LUC, which depended on LUCAS function. Novelan *et al.* [36] built up an SMS security framework for cell phone devices in utilizing TEA. [37] Proposed new tiny symmetric encryption algorithm (NTSA) that provided improved security for the transmission of text files through the IoT network by introducing supplementary dynamical key confusions for every round of encryption. In addition, Table 5 shows summery of TEA based schemes mentioned in this section. It can be concluded that TEA delivered comparatively better computational performance. However, the scope is very limited to certain applications only. Furthermore, it can be elaborated from the table that TEA based schemes do not provide robust security in general environment and cannot withstand modern security attacks.

F. A LIGHTWEIGHT BLOCK CIPHER (PRESENT)

It is a lightweight block cipher designed by [91]. The process is renowned for its 2.5x size compaction compared to advance encryption system (AES). The block size is fixed at 64-bit while key size can be 80 to 128-bits. The non-linear layer relies on a single 4-bit substitution box, primarily planned with the intent of hardware optimization. It is also defined as a new standard for lightweight cryptographic technique to be used for hardware chip efficiency and low-power consumption [92] e.g. FPGA. The comparative parameters are to use affordable slices and throughput with minimal energy usage at achievable high frequencies.

1) PRIMITIVE RESEARCH ON PRESENT SCHEMES

In [93], [94], and [95], authors worked on configuration of space investigation on FPGA devices for encryption and decryption activities in Spartan- FPGA based co-processor which was used in the encryption and decryption activities that required a sum of slices for 128-bit key lengths, separately. The authors used a storage-mode (ST) architecture with variable keys with on-the-fly (OTF) architecture to compute medium size keys to deliver good performing during ciphering [2]. Similarly, authors utilized two alternative models to generate the round keys required by the acquired algorithm. A 16-bit data-path with 128-bit key scheduling was offered to reduce latency and energy cost [13] which combines ciphering processes by using 80- and-128 bit keys for 64-bit data cipher. The design of the model was implemented by utilizing Verilog-HDL on Xilinx 14.7 platform [43]. Moreover, Two diverse RAM based executions of the design is discussed in [54]. In the primary execution, the substitution box of the block was added into the FPGA slices. In the subsequent execution, it was further pushed into the RAM. [47] presented similar execution of the PRESENT with 8-bits data which can be identified with encryption process only. The technique used Xilinx Virtex-5 device and stretched the latency and throughput at high frequency of 236.574 Mhz. Another execution utilizing a 64-bit data-path, was applied in [1] that expended the slices of Xilinx Spartan-6 FPGA device. Similar data block framework was orchestrated with respect to slice region of the Xilinx Virtex-5 FPGA device by [22] with inertness of clocks, most extreme frequency and throughput. Nevertheless, as indicated by the authors, decryption activity is somewhat unpredictable in contrast to the encryption activity. In association with one of the executions in which both encryption and decryption activities were handled In [93], accepted that in the last round, the key is accessible at the beginning of the decryption activity. They explained that the key is static in nature all through the entirety of the encryption and decryption activities for all the data blocks. Wenling Wu and Lei Zhang [96] built up L-Block scheme for lightweight applications through PRESENT. In another execution by [22], the setting was set such that the decryption activity required practically the same region as of encryption, when actualized independently. In the accompanying segment, a coordinated encryption and decryption plan was proposed and depicted in [46], where the author performed an integrated encryption and decryption process for different key sizes. Additionally, Table 6 presents summary of the mentioned lightweight PRESENT cryptographic schemes. The higher frequencies result in larger block sizes and throughput but consumed more energy. Similarly, Larger number of slices consumes less energy with high throughput. However, devices with large slices are expensive that increase operational costs of such schemes.

G. HYBRID LIGHTWEIGHT ENCRYPTION SCHEMES

Such lightweight encryption schemes are devised for domain specific IoT and M2M business applications. There are combinations of attributes used to devise extremely random ciphers and keys to deliver efficient performance costs. Research adopted random features to distinguish devices identities and mixed with private keys which are then fed to standard or non-standard lightweight hash functions to achieve maximum cost efficiency with high security.

Hossain *et al.* [49] proposed a security system that ensured user authorization and guaranteed access to resources and networks. The security structure approved a user dependent Open-ID standard. Elhoseny *et al.* [50] proposed a half breed encryption design made from combination of AES and RSA calculations. The model started by encoding the secret data then disguised the result in a dispersed image using 2D-DWT-1L and 2D-DWT-2L. In [51], authors proposed another FSFIBE methodology to guarantee integrate data transmission in M2M networks. Hence the framework was made secure without arbitrary changes. Furthermore, FSFIBE strategy provided the property of error resilience. In [53], authors proposed a technique that used spatial and

TABLE 5. Summary of mentioned TEA based lightweight techniques.

Article	Technique	Key Size	ET	DT	Achievement	Weakness
[9]	LFSR _ MTEA	192	0.346	-	Increased security	Limited time complexity
[15]	Substitution and gamma permutation	32-128	0.11-0.289	0.13 - 0.299	Process binary data	Limited scope and functionality
[23]	LEA	128-256	0.250-0.685	0.245 – 0.702	Lightweight key sizes	S-box is replaced with random number generator
[45]	WAKE / IDEA	56	-	-	Robust encryption via DES	Lack of adaptability in Feistel structure
[38]	TEA and LUCAS	32-128	0.125	0.124 - 0.126	Robust encryption	Inefficient computational cost due to uniform key size
[36]	TEA for cellular network	32-128	0.125	0.124 - 0.126	TEA for cell phones	Inefficient computational cost
[37]	NTSA	32-240	0.07 - 0.113	0.068 - 0.119	Efficient computational cost	Limited scope

^{ET}: Encryption time (ms) , ^{DT}: Decryption Time (ms)

TABLE 6. Summary of present based lightweight schemes.

Article	Tool	Technique	BS	KS	SL	T	Fr	Achievements	Weakness
[2]	Xilinx Virtex-5	PRESENT block cipher	80	128	55	26.3 Mbps	13.56 MHz	High performance encryption	Energy costs in high frequencies
[13]	Virtex-5 XC5VLX5 0T	PRESENT block cipher	80	128	67	6.38 Mbps	13.56 MHz	LUT-6 consumed less energy	Inefficient performance in LUT-6-based FPGAs
[22]	Xilinx Virtex-5 XC5VLX5 0T	PRESENT block cipher	64	47	87	341.64 Mbps	221.64 MHz	High throughput and less slices	Integral structure design issues
[43]	FPGA/ Artix-7	PRESENT block cipher	80	128	181	392 Mbps	196 MHz	High throughput at Max frequency	More energy usage in achieving high throughput
[54]	FPGA/CPL D	RAM-based PRESENT cipher executions	64	128	85	6.03 Kbps	100 KHz	Efficient throughput with less computation	Expensive memory cost
[47].	Xilinx Virtex-5 XC5VLX5 0	PRESENT block cipher	80	64	62	51.32 Mbps	236 .574 MHz	High throughput latency	Small data blocks more execution process
[1]	Xilinx Spartan-6 XC6SLX1	PRESENT block cipher	64	128	74	221.63 Mbps	221.63 MHz	High throughput and latency	Inefficient energy usage with extreme frequencies
[46]	Virtex-5 XC5VLX1 10T	PRESENT block cipher	64	128	150	410 Mbps	210 MHz	High throughput with efficient energy usage	Keys stored at BRAM are not secure

^{BS}: Block Size, ^{KS}: Key Size, ^{T}: Throughput ^{Fr}: Frequency

time slots of the user comprising processes as two constituents of authentication along unique ID procurement to adjust the security provisions and verification in M2M communications network. In [31], authors proposed a strategy for privacy safeguarding and gateway aided authorization of data in smart grids in terms of power usage. They used bloom filter and homomorphic ciphers utilized in distributed smart-meters to gateway in smart-homes. Authors in [97] presented a privacy saving and effective data recovery plan over hybrid cloud. The plan obtained prominent Map-Reduce system using information segment technique, which is free of explicit applications. Kitsos et.al [16] proposed a hardware-based execution inspection of lightweight block encryption algorithms. It reviewed about the ciphers, which are reasonable for radio frequency identification security applications. Ding et.al [6] proposed another lightweight

TABLE 7. Summary of mentioned hybrid lightweight techniques.

Article	Technique	Feature	Security	Achievement	Limitations
[6]	Hardware-based execution	Lightweight stream cipher	Strong encrypted keys	Lightweight stream and strong encrypted keys	The scope is limit to FPGA based MTC devices
[16]	FPGA based execution	Lightweight block encryption	Access control and user authorization	Radio frequency identification security	Scope limited to RFID based security applications
[31]	Bloom filter and homomorphic ciphers	Attribute based Authentication	Data confidentiality	Gateway aided secure authentication in BAN	Focused to limit power usage in smart grids
[53]	Spatial and time slots based Authentication	Unique ID procurement	User Authentication	Security provisions and verification in M2M	Symmetric and asymmetric based hybrid cryptosystem
[51]	FSFIBE	Error resilience	Access control and user authorization	Secure data transmission	Secure without arbitrary changes
[50]	Dual encryption (AES & RSA)	Medical imaging encryption	Encrypted characterized patient data	2d-DWT-2l based cryptosystem	High nuance, limited and unimportant debilitating in stego-image
[49]	SAT (Security Access Toke)	Authorization Access control	Context-aware access control model.	Improved healthcare security in hospitals	Theoretical model of healthcare IoT secure framework
[40]	User Biometric Signature	User authentication	Strong password protection	Novel password mechanism	Biometric data in sensitive devices

stream cipher family surely understood as Welch-Gong takes an 80-bit secret key and beginning vector of 80 bits as inputs. There exist Key-IV sets to produce keystreams. Additionally, Table 7 summarizes the study related to hybrid lightweight cryptosystem-based schemes, mentioned in this section. Hybrid techniques can well define a comprehensive general lightweight scheme which is why several methods have been used to improve computational performance and security. However, these techniques mainly focus on security provisions without consideration for affordable computational and memory costs for resource constrained devices.

In contrast of section 2, Table 8 represents comparative study of overall schemes in terms of features, cryptosystems, security measures and achieved milestone, mentioned in this paper. ABE based schemes offer good computational performance as asymmetric cryptography is utilized. These schemes are best suited in access control driven IoT applications that can achieve efficient computation in resource constrained M2M networks. However, the security analysis is often limited to specific scenarios and can only address basic security features. The IBC based schemes involved advanced techniques in asymmetric cryptography through dynamic third-party and dynamic private keys where third-party is used to offload and execute heavy computational tasks to improve overall efficiency in IoT network. However, securing the third-party is an extra task of the network. A DBMS based third-party is always vulnerable to database related attacks. Moreover, servers that offer assistance in challenging computation, are assumed to not suffer from modern attacks. On the other hand, ECC based schemes offer robustness and cost efficiency by involving third-party to offload heavy computation, asymmetric cryptography and countering modern security attacks in resource constrained IoT networks. Few schemes also mixed ECC with hybrid attributes to ensure adaptability and robust encryption. However, the scope is limited to specific applications and the computational efficiency can only be guaranteed if right bilinear-pairing and scaler multiplication processes are adopted. Additionally, schemes based on signcryption are lightweight with limited scope, yet are computationally very efficient and flexible for small and closed intranet network of IoT and M2M communication networks. The processes are entirely dependent on the type of encryption technique is adopted whereas certificates can be from any hybrid entity. Application specific TEA and PRESENT encryption techniques are chosen for limited chip encryption, mostly involving FPGA and SoC (System on Chip) devices. These techniques accommodate hardware-based encryption without any firmware effort hance save memory and computational power at the expense of high energy consumption. However, the scope is extremely limited to FPGA and SoC based hardware manufacturers. The hybrid schemes provide vast variety of techniques. Similarly, the public and private keys are defined from a variety of user and device attributes. Consequently, the hybrid lightweight schemes achieved tough security, cost-effective performance, and affordable energy consumption. However, hybrid schemes have high limitations in application-based schemes. There are few schemes which are adaptive to other application environments.

Additionally, based on Table 8, Figure 6 presents taxonomy of lightweight cryptographic types and techniques used in M2M and IoT networks. The taxonomy can help a novel study

TABLE 8. Analysis of overall mentioned lightweight schemes.

Types	Features	CR	Performance Measurements	SA	Challenges	REF
ABE	• Access Control • Efficient computation performance	•S •A	• Complexity • Computation	• BS • SS	• Analysis in advance security threats • Alternative approach to bilinear pairing	[7] [10] [18]
IBC	• Public Key Cryptography • Private Key Generators	•A •H	• Cryptographic computations • PKG analysis	• MST	• Key Secrecy • PKG Security • Third Party security analysis	[19-21]
ECC	• Public Key Cryptography • Private Key Generator • Bilinear Pairing • Curve Types	•A •H	• Network overhead • Cryptographic computations • PKG analysis • Key Secrecy	• MST	• Key Secrecy • PKG Security • Network Overhead • Curve Efficiency	[27-29]
Signcryption	• Certificate • Encryption Technique	•S •A •H	• Computation & Communication cost	• BS • FBS	• Computational Efficiency • Forward secrecy • Network adaptability	[32-34]
TEA	• Memory Utilization • Computation	•S •H	• Space complexity • Permutations • Time complexity	• BS	• Block Size • Computational efficiency	[36-38]
PRESENT	• Chip Region • Hardware-based Execution	•H	• Slice Size • Key Size • Throughput • Frequency	• BS	• Energy usage • Region Issues • Extreme frequencies	[1, 46, 47]
Hybrid	• Encryption • Improved computational complexity	•H	• Computational & • Communication Efficiency	• MST	• Limited Scope • Adaptability • Scalability	[49-51]

^{CR} Cryptosystem, ^{S} Symmetric, ^{A} Asymmetric, ^{H} Hybrid, ^{SA} Security Analysis, ^{BS} Basic Security, ^{MST} Modern Security Threats, ^{SS} Selective Security, ^{FBS} Forward, Backward Secrecy

on lightweight cryptography to get a basic idea of current popular techniques being used including the main challenges in particular field.

III. CHALLENGES

This section emphasizes on issues, challenges and open research areas related to lightweight cryptographic techniques presented in this article. The discussed numerous lightweight cryptographic techniques utilized for resource constrained MTC devices in this paper, summarized several types of techniques utilized in different approaches to address lightweight algorithms for general and specific applications. However, most of the discussed lightweight cryptographic schemes lack in providing either robust security against modern attacks or do not possess the capability to be applied on resource constrained CPS, IoT and MTC device. Issues found in mentioned schemes in this article are mentioned in the following,

A. ISSUES

The challenges are addressed in the following:

1) Though ABE schemes provide efficient computation during encryption but lack in resilient security against modern attacks. A scheme that incorporates resilient security in ABE schemes could highly improve the impact of ABE in resource constrained MTC devices and CPS.
2) The cryptographic applications examined in this paper aid to exhibit the overall performance of several lightweight cryptographic schemes. Consequently, it is vital to adopt a novel solution and propose a general standardized cryptographic model, that should be comparatively analyzed with the current ones. The standardized cryptography could help in quality improvement of the research in lightweight cryptographies for M2M communication networks' flexibility due to fewer system resources [98]. This also points to the importance of limited security metrics. To the best of our knowledge, no security metric can accurately estimate cryptographic security efficiency whereas encryption is subjected to decoding which is intended to break the encoded MAC by series of attacks. However, current lightweight security schemes need improvements in analyzing security against newly devised attacks.
3) In Current PKI systems, that include ECC, Hybrid, TEA and Signcryption; private keys are typically created on the user's end that causes issue of implicit

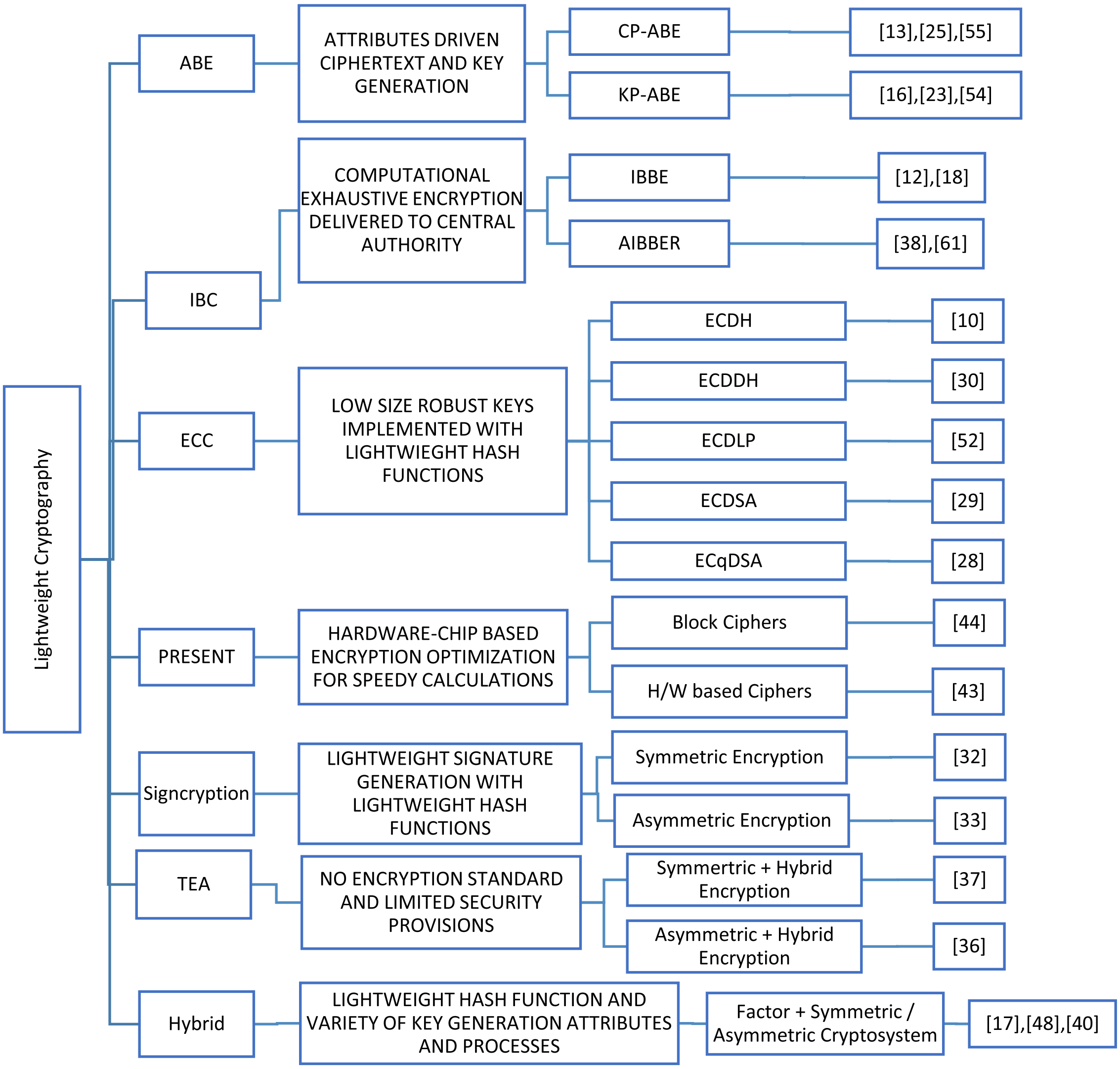
Lightweight Cryptography
ABE
ATTRIBUTES DRIVEN CIPHERTEXT AND KEY GENERATION
CP-ABE
[13],[25],[55]
KP-ABE
[16],[23],[54]
IBC
COMPUTATIONAL EXHAUSTIVE ENCRYPTION DELIVERED TO CENTRAL AUTHORITY
IBBE
[12],[18]
AIBBER
[38],[61]
ECC
LOW SIZE ROBUST KEYS IMPLEMENTED WITH LIGHTWIEGHT HASH FUNCTIONS
ECDH
[10]
ECDDH
[30]
ECDLP
[52]
ECDSA
[29]
ECqDSA
[28]
PRESENT
HARDWARE-CHIP BASED ENCRYPTION OPTIMIZATION FOR SPEEDY CALCULATIONS
Block Ciphers
[44]
H/W based Ciphers
[43]
Signcryption
LIGHTWEIGHT SIGNATURE GENERATION WITH LIGHTWEIGHT HASH FUNCTIONS
Symmetric Encryption
[32]
Asymmetric Encryption
[33]
TEA
NO ENCRYPTION STANDARD AND LIMITED SECURITY PROVISIONS
Symmertric + Hybrid Encryption
[37]
Asymmetric + Hybrid Encryption
[36]
Hybrid
LIGHTWEIGHT HASH FUNCTION AND VARIETY OF KEY GENERATION ATTRIBUTES AND PROCESSES
Factor + Symmetric / Asymmetric Cryptosystem
[17],[48],[40]

FIGURE 3. Taxonomy of lightweight cryptographic approaches in M2M communication.

key escrow. While several different schemes proposed removal of key escrow including secure keys, secret sharing, certificate-based and certificate-less cryptography. However, many attempted to shift to dynamic keys which typically result in exhaustive memory and computational. Thus, a novel efficient way of private key escrow is very challenging.

4) A resource-constrained device's security level is flexible due to fewer system resources [98]. This points to the importance of limited security metrics. To the best of our knowledge, no security metric can accurately estimate cryptographic security efficiency whereas encryption is subjected to decoding which is intended to break the encoded MAC by series of attacks. However, current lightweight security schemes need improvements in analyzing security against newly devised attacks.

In Current PKI systems, that include ECC, Hybrid, TEA and Signcryption; private keys are typically created on the user's end that causes issue of implicit key escrow. While several different schemes proposed removal of key escrow including secure keys, secret sharing, certificate-based and certificate-less cryptography. However, many attempted to alter to dynamic keys that typically resulted in exhaustive memory and computation.

Thus, a faster and more secure adoption of private key escrow is very challenging.

B. OPPORTUNITIES

Lightweight cryptography development is utmost needed in current market of IoT and M2M communication. The mentioned study of several lightweight techniques offers several deliverable opportunities and future directions to enhance performance, cost and to ensure further robustness of security. The research opportunities are the following,

1) Identity-based, ECC and TEA schemes have indistinguishable problems in operations. Such as if A and

B use a secure system to send messages. Since the data required to discover A's public-key, is calculated by A's ID and shared public key. It is impossible to cancel A's identifications and produce new identifications without changing A's ID or the shared public key and creating new private keys to B and other users. Thus, a network-based key that portrays statistically undiscoverable attributes of network is a challenging yet adaptive opportunity. Network-based key refers to a shared public key that changes over certain timestamps. This type of change should be decodable for all the connected devices. Similarly, network-based key should also produce a large random unique number once it coincides with device's private keys. Thus the entire network will use two keys only for encrypted message transmission which can vastly decrease memory use and generating more dynamic keys for strong security.

2) The key size and block size plays vital role in the improvement of lightweight cryptographic schemes for resource constrained devices. Increase in the key size results increase in ciphertext hence it increases requirement of intense computational power. Similar can be said for the block ciphers. Thus, balancing security and efficiency becomes a challenge. Numerous countermeasures are implemented to prevent modern attacks but new attacks can overwhelm the implemented measures in preventing known attacks [99]. In this regard, the encryption capability is greatly needed that can show comprehensive resilience against all modern attacks efficiently. Additionally, TEA, XTEA and other similar less computational costly techniques can be introduced to decrease key sizes which can further decease the overall block sizes of ciphered texts. The challenge lies in designing very strong keys that should withstand several heavy statistical attacks.
3) Since signcryption offers data confidentiality including authentication and data integrity with efficient performance thus there is a steep gap of engaging signcryption in mainstream security provision in industrial internet of things (IIoTs) and autonomous MTC devices as signcryption is mostly neglected to provide vigorous security in more generalized IoT applications. Devices in IIoTs can use signcryption certificates as private keys. Then these certificates could be used to verify an IoT device itself. This type of self-verification technique can decrease computational overhead of each IoT device and consequently improve performance of the entire network.
4) If PKG (Private Key generator); used in ECC, IBE Signcryption and Hybrid cryptosystems) is compromised, data protected over the period of keypair (public/private) used by the third party, will also be compromised. It marks PKG a high value target to attackers. Thus, the third-party private-key generators can be made more robust using strong ECC curves for security improvements.
5) Implementation of simulated schemes in Signcryption, XTEA and ECC with inclusion of mutual authentication and then comparing the performance, cost and power analysis can offer thorough understanding of encryption robustness and communication cost efficiency. The presented lightweight schemes focused mainly on encryption. However, involving mutual authentication process between the sender and receiver device will further improve security with minimal cost.

IV. CONCLUSION

A comprehensive study is presented on lightweight cryptographic schemes for resource constrained autonomous MTC devices in M2M communication networks. The study covered a wide range of different types of lightweight cryptographic techniques implemented to achieve strong security, resourcefulness, efficient performance, and adaptability for different IoT applications. Moreover, each type of lightweight cryptography offers study on similar recent schemes and provides a comparative study in related Tables. The study also presented an overall summarized analysis of different types of schemes mentioned in this paper in terms of related security and performance features that a lightweight cryptographic scheme requires, as shown in Table 8. Additionally, a taxonomy of lightweight cryptography in M2M communication is presented in Figure 3. Furthermore, the article discusses several issues commonly found in the covered lightweight cryptography studies and offers adaptable solutions for future developments.

CONFLICT OF INTERESTS

The authors concur that there is no conflict of interests.

ACKNOWLEDGMENT

Tulha Moaiz Yazdani would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project R-2022-84.

REFERENCES

[1] C. A. Lara-Nino, M. Morales-Sandoval, and A. Diaz-Perez, "Novel FPGA-based low-cost hardware architecture for the PRESENT block cipher," in *Proc. Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2016, pp. 646–650.

[2] R. Chatterjee and R. Chakraborty, "A modified lightweight PRESENT cipher for IoT security," in *Proc. Int. Conf. Comput. Sci., Eng. Appl. (ICCSEA)*, Mar. 2020, pp. 1–6.

[3] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in *Big Data and Internet of Things, A Roadmap for Smart Environments*. Cham, Switzerland: Springer, 2014, pp. 169–186.

[4] A. Lohachab and Karambir, "ECC based inter-device authentication and authorization scheme using MQTT for IoT networks," *J. Inf. Secur. Appl.*, vol. 46, pp. 1–12, Jun. 2019.

[5] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative ciphertext policy attribute-based encryption for the Internet of Things," in *Proc. Int. Conf. Adv. Netw. Distrib. Syst. Appl.*, Jun. 2014, pp. 64–69.

[6] L. Ding, C. Jin, J. Guan, and Q. Wang, "Cryptanalysis of lightweight WG-8 stream cipher," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 645–652, Apr. 2014.

[7] L. Touati and Y. Challal, "Collaborative KP-ABE for cloud-based Internet of Things applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–7.

[8] A. Kumar, R. Saha, M. Alazab, and G. Kumar, "A lightweight signcryption method for perception layer in Internet-of-Things," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102662.

[9] M. Abdelhalim, M. El-Mahallawy, M. Ayyad, and A. Elhennawy, "Design and implementation of an encryption algorithm for use in RFID system,," *Int. J. RFID Secur. Cryptogr. (IJRFIDSC)*, vol. 1, nos. 1–2, pp. 15–22, 2012.

[10] N. Oualha and K. T. Nguyen, "Lightweight attribute-based encryption for the Internet of Things," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–6.

[11] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st, Ed., MCC Workshop Mobile cloud Comput. (MCC)*, 2012, pp. 13–16.

[12] K. N. Prasetyo, Y. Purwanto, and D. Darlis, "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICoICT)*, May 2014, pp. 75–79.

[13] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight hardware architectures for the present cipher in FPGA," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 9, pp. 2544–2555, Sep. 2017.

[14] M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez, and P. Schwabe, "High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers," *Des., Codes Cryptogr.*, vol. 77, nos. 2–3, pp. 493–514, Dec. 2015.

[15] O. N. Zhdanov and A. V. Sokolov, "Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic," *Far East J. Electron. Commun.*, vol. 16, no. 3, pp. 573–589, Sep. 2016.

[16] P. Kitsos, N. Sklavos, M. Parousi, and A. N. Skodras, "A comparative study of hardware architectures for lightweight block ciphers," *Comput. Electr. Eng.*, vol. 38, no. 1, pp. 148–160, Jan. 2012.

[17] S. Hussain, I. Ullah, H. Khattak, M. A. Khan, C.-M. Chen, and S. Kumari, "A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for industrial Internet of Things (IIoT)," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102625.

[18] S. F. S. Adnan, M. A. M. Isa, and H. Hashim, "Timing analysis of the lightweight AAβ encryption scheme on embedded Linux for Internet of Things," in *Proc. IEEE Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, May 2016, pp. 113–116.

[19] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Cham, Switzerland: Springer, 2016, pp. 223–239.

[20] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Efficient semi-static secure broadcast encryption scheme," in *Proc. Int. Conf. Pairing-Based Cryptogr.*, Cham, Switzerland: Springer, 2013, pp. 62–76.

[21] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Cham, Switzerland: Springer, 2009, pp. 171–188.

[22] N. Hanley and M. ONeill, "Hardware comparison of the ISO/IEC 29192-2 block ciphers," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Aug. 2012, pp. 57–62.

[23] *128 Bit Light Weight Block Cipher LEA*, Information Telecommunication Organization Standard (Korean Standard), Knowledge Translation and Transfer (KTT) Association, Geneva, Switzerland, 2013.

[24] R. de Clercq, L. Uhsadel, A. Van Herrewege, and I. Verbauwhede, "Ultra low-power implementation of ECC on the ARM Cortex-M0+," in *Proc. 51st Annu. Design Autom. Conf. Design Autom. Conf. (DAC)*, 2014, pp. 1–6.

[25] L. Touati and Y. Challal, "Efficient CP-ABE attribute/key management for IoT applications," in *Proc. IEEE Int. Conf. Comput. Inf. Technol.; Ubiquitous Comput. Commun.; Dependable, Autonomic Secure Comput., Pervasive Intell. Comput.*, Oct. 2015, pp. 343–350.

[26] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[27] G. U. Devi, E. V. Balan, M. K. Priyan, and C. Gokulnath, "Mutual authentication scheme for IoT application," *Indian J. Sci. Technol.*, vol. 8, no. 26, p. 15, Oct. 2015.

[28] D. Chu, J. Großschädl, Z. Liu, V. Müller, and Y. Zhang, "Twisted edwards-form elliptic curve cryptography for 8-bit AVR-based sensor nodes," in *Proc. 1st ACM Workshop Asia Public-Key Cryptogr. (AsiaPKC)*, 2013, pp. 39–44.

[29] S. R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho, "Performance analysis of end-to-end security schemes in healthcare IoT," *Proc. Comput. Sci.*, vol. 130, pp. 432–439, Jan. 2018.

[30] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015.

[31] T. W. Chim, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Trans. Depend. Secure Comput.*, vol. 12, no. 1, pp. 85–97, Jan. 2015.

[32] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[33] M. Zia and R. Ali, "Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls," *PLoS ONE*, vol. 13, no. 12, Dec. 2018, Art. no. e0208857.

[34] W. Iqbal, M. Afzal, and F. Ahmad, "An efficient elliptic curve based signcryption scheme for firewalls," in *Proc. 2nd Nat. Conf. Inf. Assurance (NCIA)*, Dec. 2013, pp. 67–72.

[35] J. Cao, M. Ma, and H. Li, "GBAAM: Group-based access authentication for MTC in LTE networks," *Secur. Commun. Netw.*, vol. 8, no. 17, pp. 3282–3299, Nov. 2015.

[36] M. S. Novelan, A. M. Husein, M. Harahap, and S. Aisyah, "SMS security system on mobile devices using tiny encryption algorithm," *J. Phys., Conf. Ser.*, vol. 1007, Apr. 2018, Art. no. 012037.

[37] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019.

[38] D. Rachmawati, A. Sharif, and M. A. Budiman, "Hybrid cryptosystem using tiny encryption algorithm and LUC algorithm," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 300, no. 1, 2018, Art. no. 012042.

[39] C. G. Thorat and V. S. Inamdar, "Implementation of new hybrid lightweight cryptosystem," *Appl. Comput. Informat.*, vol. 16, nos. 1–2, pp. 195–206, May 2018.

[40] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.

[41] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "Cryptographic key generation using ECG signal," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 1024–1031.

[42] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, and I. You, "TTP based high-efficient multi-key exchange protocol," *IEEE Access*, vol. 4, pp. 6261–6271, 2016.

[43] H. D. Azari and P. V. Joshi, "An efficient implementation of present cipher model with 80 bit and 128 bit key over FPGA based hardware architecture," *Int. J. Pure Appl. Math.*, vol. 119, no. 14, pp. 1825–1832, 2018.

[44] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Elsevier Future Generat. Comput. Syst.*, vol. 49, pp. 104–112, Aug. 2015.

[45] D. Abdullah, R. Rahim, A. P. Utama Siahaan, A. F. Ulva, Z. Fitri, M. Malahayati, and H. Harun, "Super-encryption cryptography with IDEA and WAKE algorithm," *J. Phys., Conf. Ser.*, vol. 1019, Jun. 2018, Art. no. 012039.

[46] J. G. Pandey, T. Goel, and A. Karmakar, "A high-performance and area-efficient VLSI architecture for the PRESENT lightweight cipher," in *Proc. 31st Int. Conf. VLSI Design 17th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2018, pp. 392–397.

[47] J. J. Tay, M. L. D. Wong, M. M. Wong, C. Zhang, and I. Hijazin, "Compact FPGA implementation of PRESENT with Boolean S-box," in *Proc. 6th Asia Symp. Quality Electron. Design (ASQED)*, Aug. 2015, pp. 144–148.

[48] Z. Liu, H. Seo, J. Grosschadl, and H. Kim, "Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1385–1397, Jul. 2016.

[49] M. Hossain, S. M. R. Islam, F. Ali, K.-S. Kwak, and R. Hasan, "An Internet of Things-based health prescription assistant and its security system design," *Future Gener. Comput. Syst.*, vol. 82, pp. 422–439, May 2018.

[50] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[51] E. R. Naru, H. Saini, and M. Sharma, ''A recent review on lightweight cryptography in IoT,'' in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Feb. 2017, pp. 887–890.

[52] N. W. Hundera, Q. Mei, H. Xiong, and D. M. Geressu, ''A secure and efficient identity-based proxy signcryption in cloud data sharing,'' *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 1, pp. 455–472, 2020.

[53] H. Zhu, X. Lin, Y. Zhang, and R. Lu, ''Duth: A user-friendly dual-factor authentication for Android smartphone devices,'' *Secur. Commun. Netw.*, vol. 8, no. 7, pp. 1213–1222, May 2015.

[54] E. B. Kavun and T. Yalcin, ''RAM-based ultra-lightweight FPGA implementation of PRESENT,'' in *Proc. Int. Conf. Reconfigurable Comput. (FPGAs)*, Nov. 2011, pp. 280–285.

[55] M. Nawari, H. Ahmed, A. Hamid, and M. Elkhidir, ''FPGA based implementation of elliptic curve cryptography,'' in *Proc. World Symp. Comput. Netw. Inf. Secur. (WSCNIS)*, Sep. 2015, pp. 1–8.

[56] H. Fujii and D. F. Aranha, ''Efficient Curve25519 implementation for ARM microcontrollers,'' in *Proc. Anais Estendidos do XVIII Simpósio Brasileiro em Segurança da Informaço e de Sistemas Computacionais (SBC)*, 2018, pp. 57–64.

[57] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, and E. Ayday, ''A survey on information security threats and solutions for machine to machine (M2M) communications,'' *J. Parallel Distrib. Comput.*, vol. 109, pp. 142–154, Nov. 2017.

[58] L. Touati and Y. Challal, ''Batch-based CP-ABE with attribute revocation mechanism for the Internet of Things,'' in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 1044–1049.

[59] H. Guo and L. Deng, ''An identity based proxy signcryption scheme without pairings,'' *Int. J. Netw. Secur.*, vol. 22, no. 4, pp. 561–568, 2020.

[60] F. Li, Z. Zheng, and C. Jin, ''Secure and efficient data transmission in the Internet of Things,'' *Telecommun. Syst.*, vol. 62, no. 1, pp. 111–122, 2016.

[61] C. Hahn, H. Kwon, and J. Hur, ''Toward trustworthy delegation: Verifiable outsourced decryption with tamper-resistance in public cloud storage,'' in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 920–923.

[62] N. C. Kumar, A. Basit, P. Singh, and V. Ch. Venkaiah, ''Lightweight cryptography for distributed PKI based MANETS,'' 2018, *arXiv:1804.06313*.

[63] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. García, ''Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things,'' *Sensors*, vol. 20, no. 2, p. 501, Jan. 2020.

[64] Y. Mao, J. Li, M.-R. Chen, J. Liu, C. Xie, and Y. Zhan, ''Fully secure fuzzy identity-based encryption for secure IoT communications,'' *Comput. Standards Interfaces*, vol. 44, pp. 117–121, Feb. 2016.

[65] K. L. Tsai, Y. L. Huang, F. Y. Leu, J. S. Tan, and M. Ye, ''High-efficient multi-key exchange protocol based on three-party authentication,'' in *Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2014, pp. 487–492.

[66] A. Barki, A. Bouabdallah, S. Gharout, and J. Traoré, ''M2M security: Challenges and solutions,'' *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1241–1254, 2nd Quart., 2016.

[67] M. Saleh, N. Jhanjhi, A. Abdullah, and R. Saher, ''Proposing encryption selection model for IoT devices based on IoT device design,'' in *Proc. 23rd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2021, pp. 210–219.

[68] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K.-K. R. Choo, ''Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment,'' *Comput. Stand. Interfaces*, vol. 54, no. P1, pp. 3–9, Nov. 2017.

[69] V. Rao and K. Prema, ''A review on lightweight cryptography for Internet-of-Things based applications,'' *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 9, pp. 8835–8857, 2020.

[70] S. Ding, C. Li, and H. Li, ''A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT,'' *IEEE Access*, vol. 6, pp. 27336–27345, 2018.

[71] S. W. Shah and S. S. Kanhere, ''Recent trends in user authentication—A survey,'' *IEEE Access*, vol. 7, pp. 112505–112519, 2019.

[72] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, ''Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities,'' *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[73] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Cham, Switzerland: Springer, 2005, pp. 457–473.

[74] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ''Attribute-based encryption for fine-grained access control of encrypted data,'' in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 89–98.

[75] Y. Dodis and N. Fazio, ''Public key broadcast encryption for stateless receivers,'' in *Proc. ACM Workshop Digit. Rights Manage.*, Cham, Switzerland: Springer, 2002, pp. 61–80.

[76] C. Delerablée, ''Identity-based broadcast encryption with constant size ciphertexts and private keys,'' in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT)*, Springer, 2007, pp. 200–215.

[77] R. Sakai and J. Furukawa, ''Identity-based broadcast encryption,,'' *IACR Cryptol. ePrint Arch.*, vol. 2007, p. 217, Jan. 2007.

[78] M. Green, S. Hohenberger, and B. Waters, ''Outsourcing the decryption of abe ciphertexts,'' in *Proc. USENIX Secur. Symp.*, 2011, p. 34.

[79] Z. Liu, E. Wenger, and J. Großschädl, ''MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks,'' in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, Cham, Switzerland: Springer, 2014, pp. 361–379.

[80] G. Hinterwälder, A. Moradi, M. Hutter, P. Schwabe, and C. Paar, ''Full-size high-security ECC implementation on MSP430 microcontrollers,'' in *Proc. Int. Conf. Cryptol. Inf. Secur. Latin Amer.*, Cham, Switzerland: Springer, 2014, pp. 31–47.

[81] E. Wenger, T. Unterluggauer, and M. Werner, ''8/16/32 shades of elliptic curve cryptography on embedded processors,'' in *Proc. Int. Conf. Cryptol. India*, Cham, Switzerland: Springer, 2013, pp. 244–261.

[82] M. Hutter and P. Schwabe, ''NaCl on 8-bit AVR microcontrollers,'' in *Proc. Int. Conf. Cryptol. Afr.*, Cham, Switzerland: Springer, 2013, pp. 156–172.

[83] C. P. L. Gouvêa, L. B. Oliveira, and J. López, ''Efficient software implementation of public-key cryptography on sensor networks using the MSP430X microcontroller,'' *J. Cryptograph. Eng.*, vol. 2, no. 1, pp. 19–29, May 2012.

[84] D. F. Aranha, R. Dahab, J. López, and L. B. Oliveira, ''Efficient implementation of elliptic curve cryptography in wireless sensors,'' *Adv. Math. Commun.*, vol. 4, no. 2, pp. 169–187, May 2010.

[85] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, ''Comparing elliptic curve cryptography and RSA on 8-bit CPUs,'' in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Cham, Switzerland: Springer, 2004, pp. 119–132.

[86] A. Liu and P. Ning, ''TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,'' in *Proc. Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2008, pp. 245–256.

[87] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, ''NanoECC: Testing the limits of elliptic curve cryptography in sensor networks,'' in *Proc. Eur. Conf. Wireless Sensor Netw.*, Cham, Switzerland: Springer, 2008, pp. 305–320.

[88] M. Toorani and A. A. Beheshti, ''Cryptanalysis of an elliptic curve-based signcryption scheme,'' 2010, *arXiv:1004.3521*.

[89] K. Grindrod, H. Khan, U. Hengartner, S. Ong, A. G. Logan, D. Vogel, R. Gebotys, and J. Yang, ''Evaluating authentication options for mobile health applications in younger and older adults,'' *PLoS ONE*, vol. 13, no. 1, Jan. 2018, Art. no. e0189048.

[90] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, ''A robust and energy efficient authentication protocol for industrial Internet of Things,'' *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018.

[91] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, ''PRESENT: An ultra-lightweight block cipher,'' in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Cham, Switzerland: Springer, 2007, pp. 450–466.

[92] J. M. Carracedo, M. Milliken, P. K. Chouhan, B. Scotney, Z. Lin, A. Sajjad, and M. Shackleton, ''Cryptography for security in IoT,'' in *Proc. 5th Int. Conf. Internet Things: Syst., Manage. Secur.*, Oct. 2018, pp. 23–30.

[93] M. Sbeiti, M. Silbermann, A. Poschmann, and C. Paar, ''Design space exploration of present implementations for FPGAS,'' in *Proc. 5th Southern Conf. Program. Log. (SPL)*, Apr. 2009, pp. 141–145.

[94] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, ''Ultra-lightweight implementations for smart devices-security for 1000 gate equivalents,'' in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, Berlin, Germany: Springer, 2008, pp. 89–103.

[95] P. Yalla and J.-P. Kaps, ''Lightweight cryptography for FPGAs,'' in *Proc. Int. Conf. Reconfigurable Comput. (FPGAs)*, Dec. 2009, pp. 225–230.

[96] W. Wu and L. Zhang, ''LBlock: A lightweight block cipher,'' in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, Cham, Switzerland: Springer, 2011, pp. 327–344.

[97] Z. Zhou, H. Zhang, X. Du, P. Li, and X. Yu, "Prometheus: privacy-aware data retrieval on hybrid cloud," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2643–2651.

[98] T. Hayajneh, R. Doomun, G. Al-Mashaqbeh, and B. J. Mohd, "An energy-efficient and security aware route selection protocol for wireless sensor networks," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2015–2038, Nov. 2014.

[99] S. Bhunia, M. Abramovici, D. Agrawal, P. Bradley, M. S. Hsiao, J. Plusquellic, and M. Tehranipoor, "Protection against hardware trojan attacks: Towards a comprehensive solution," *IEEE Design Test*, vol. 30, no. 3, pp. 6–17, Jun. 2013.

SHAFI ULLAH received the B.S. and M.S. degrees in computer engineering from the Balochistan University of Information Technology, Engineering and Management Sciences, Pakistan, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree in computing with Universiti Teknologi Malaysia. He is currently working in areas under secure and reliable communications in M2M and WSN with Majmaah University, Saudi Arabia. He has published more than 700 research articles in different well-reputed international journals. His research interests include rule-based algorithm designs, mathematical modeling, analytical and computational fluid dynamics, bio-mathematics, and numerical computing.

RAJA ZAHILAH RADZI (Member, IEEE) received the Dr.Eng. degree in electrical and information system from Osaka Prefecture University, Japan, in 2012, and the B.Eng. degree in computer engineering and the M.Eng. degree in electronics and telecommunications from the Faculty of Electrical Engineering, Universiti Teknologi Malaysia (UTM). She is currently a Senior Lecturer with the Faculty of Engineering, School of Computing, UTM. Her research interests include the Internet of Things, blockchain, security, IP over WDM networks, software define networking, wireless networks, and embedded systems.

TULHA MOAIZ YAZDANI is currently working as a Lecturer with the Department of Electrical Engineering, College of Engineering, Majmaah University, Al-Majmaah, Saudi Arabia. He has published several articles in prestigious journals. His research interests include artificial neural networks, cryptographies, and machine type.

ALI ALSHEHRI received the Ph.D. degree from Oakland University, Rochester, MI, USA, in 2019. He is currently an Assistant Professor in computer science with Tabuk University, Tabuk, Saudi Arabia. His research interests include information security, web services, mobile security, network security, privacy, intrusion detection and prevention, cryptography, the IoT, and digital forensics.

ILYAS KHAN received the Ph.D. degree in applied mathematics from Universiti Teknologi Malaysia (UTM), Johor Barhu, Skudai, Malaysia. He has over 15 years of academic experience in different reputed institutions of the world. He is currently working as an Associate Professor with the Department of Mathematics, College of Science in Zulfi, Majmaah University, Saudi Arabia. He has published more than 800 research articles in top-ranked reputed journals. He is a top one-ranked Distinguish Researcher with Majmaah University and ranked five in the whole kingdom. His areas of research interests include mathematical modeling, analytical and computational fluid dynamics, bio-mathematics, and numerical computing.