Systematic Literature Review of Security Schemes for Data Exchange in Wireless Sensor Network

Shahwar Ali[1], Humaira Ashraf[1], Ata Ullah[2], and NZ Jhanjhi [3]

[1]Department of Computer Science and Software Engineering, International Islamic University
[2]Department of Computer Science, National University of Modern Languages
[3]Affiliation not available

January 10, 2024

Systematic Literature Review of Security Schemes for Data Exchange in Wireless Sensor Network

Shahwar Ali[1] , Humaira Ashraf[1], Ata Ullah[2], NZ Jhanjhi[3]

[1] Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan. {shahwarali22@gmail.com; humaira.ashraf@iiu.edu.pk }
[2] Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan. {aullah@numl.edu.pk}
[3] School of Computer Science, SCS, Taylor's University, Subang Jaya, Malaysia. {noorzaman.jhanjhi@taylors.edu.my }

Abstract - Wireless Sensor Networks (WSN) are comprised of many sensing devices that can exchange data for monitoring and tracking. Data is exchanged over different paths where a few of malicious nodes may exist to capture the data. To handle this issue, several data security schemes have been presented that are discussed in the literature. In this paper, we perform a Systematic Literature Review (SLR) to analyse existing schemes for data security in WSN as per the research question. It involves an inclusion and exclusion criteria for article selection. In literature, we explore the energy efficient schemes in the category of elliptic curve, AES, RSA, chaotic maps, efficient block ciphers, and various other techniques. These schemes are also evaluated in terms of key sizes, plain text sizes, and dominating features of related techniques and results. We identified that most of the data security schemes are extensive due to extensive computations and delayed responses. This work focuses various types of data security approaches that are compared to examine which can be more suitable for secure data exchange.

Keywords: WSN, Cryptography, Data Security, Systematic Literature Review (SLR)

I. INTRODUCTION

WSN is a scalable network with several sensor node types, such as sink node, BS (Base Station), sensor nodes, and cluster - head. The information is sent to the cluster node from the sensor node, and is then forwarded to BS for advanced communication. In various contexts, sensor nodes are used to sense and relay data. The sensor nodes can perform neighbour node detection, clever sensing, data secrecy target surveillance, mapping, node localization, synchronisation, and effective routing between nodes and base stations in several real-time packages[1]. Sensor nodes have minimal computational, memory and power capacity [2], raising the probability of vulnerabilities to security attacks.

Data security is a complicated field of study in which information is transmitted over an insecure network. In order to encrypt data, various methods were suggested; nonetheless, cryptography is one of the most reliable approaches used to secure data. In turning the original data into meaningless data, cryptographic techniques aid. Symmetric and asymmetric are two main cryptographic techniques, of which the former uses only single key for data encryption and decryption. It consumes less energy and memory. The above uses two keys, where the personal key is used for decryption and encryption is carried out by the public key. Owing to the use of two keys, the asymmetric cryptographic solution is much more reliable than symmetric. In contrast, the generation of two keys causes high energy, time, and memory consumption. Cryptographic algorithms can be used to translate plaintext into cipher text using bit-by-bit fashion in either block or stream cyphers. Later, the plain text is divided into blocks. In WSNs, data protection is also a major concern, as data flows over sensor nodes, which may be vulnerable to numerous attacks that falsify or modify transit data.

Secure data transmission is a major issue in WSN, since over the network there exists many attackers, which can attack or forge the data. Furthermore, Section 3 explores a detailed description of these articles. In order to tackle data protection in WSN, there is a considerable amount of study carried out. This article provides a study of WSN computer protection mechanisms in which our major contributions are as follows.;

1) SLR is conducted to examine the current data protection schemes in WSN and to define a loophole for further study.
2) As per the study issue, many similar data protection mechanisms are searched and closely analysed to determine strengths and vulnerabilities. First, to validate the linkage of the paper to the research question, content assessment is carried out. It is of the opinion that the papers address only data encryption systems or routing for secure data sharing in combination with them.
3) Inclusion and exclusion requirements are applicable to the collection of papers by undertaking primary and inferior tests..

The remainder of the article is broken down as follows: Section 2 discusses the Systematic Literature Analysis, where each study process is addressed. Section 3 provides a literature analysis of the papers reviewed. Section 4 introduces this survey's safety review and Section 5 completes our work.

SYSTEMATIC LITERATURE REVIEW

SLR is a type of literature reviews that practices systematic approaches to collect secondary data. SLR helps to discover, categorise, and explore the existing literature to any specific research question. Its focus is to search the relevant literature available for a specific research question. It apples extreme exclusion and inclusion criteria to find literature gap for which a suitable solution can be specified [8]. Figure 1 illustrates an overview of all the steps of SLR where abstract and introduction are in step 1 and 2. In step 3, a research question is defined which is base for further research. After that, multiple steps are followed in order to identify which research article needs to study further. After following these steps, a literature review can

be formed to perform research question-based analysis. We have identified following research question.

Question: How data can be securely exchanged while avoiding high computations with efficient response?

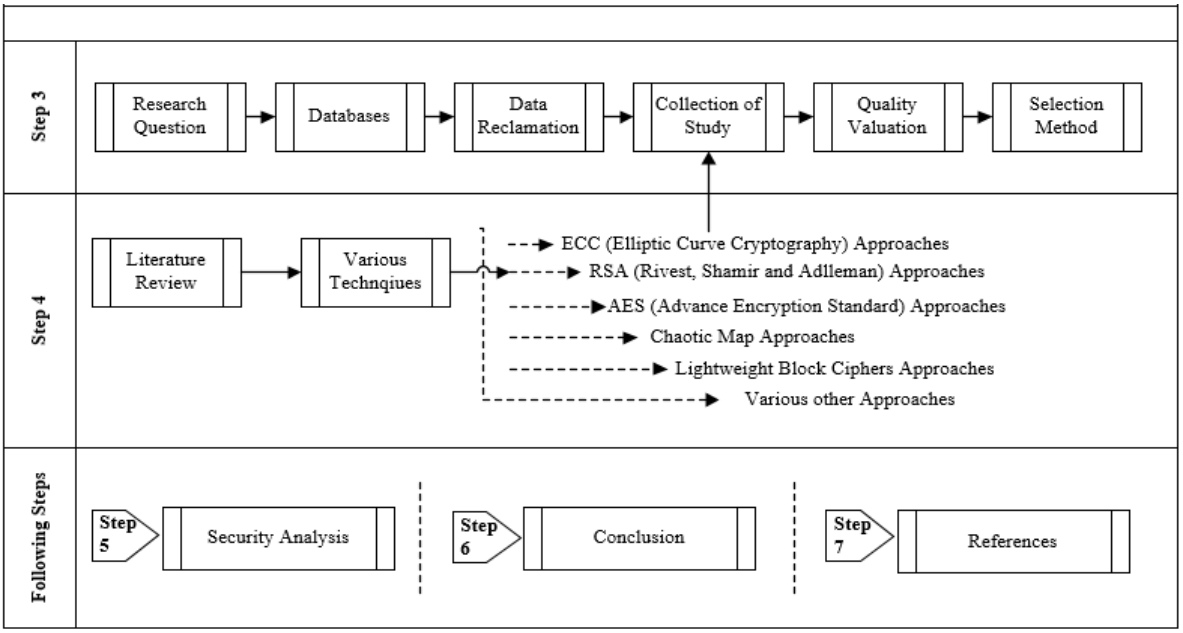

Fig. 1. Overview of SLR

A. Repositories and Data Reclamation

Digital Libraries used for searching include Science Direct (www.sciencedirect.com/), IEEE (www.ieeexplore.ieee.org/), Springer (www.springerlink.com/) and https://scholar.google.com.pk/. We have used following phrases for searching; ((“Data Security in WSN” **OR** “Data Encryption in WSN” **OR** “Text Data Security in WSN” **AND** (“secure data” **OR** “data security using chaotic map” **OR** “data security using AES” **OR** “data security using ECC” **OR** “hybrid data security”))).

B. Quality Valuation and Selection Method

This section explores the requirements to select a research article. Few quality tests are performed before the selection of any articles. Table 1 explores the ranking criteria and Table 2 illustrates the ranks and points for quality evaluation. Each paper is rated as per its relevancy with research question. Quality valuation of each article is based on the following question.

“Does the article give a solution for data security in WSN?”

TABLE 1: QUALITY EVALUATION MEASUREMENTS

Rules	Rank	Points	Quality Evaluation
None	0	0	Low
Routing Protocol	1	1	Average
Data Security Algorithm	2	1.5	Decent
Data Security + Routing	3	2	Outstanding

After defining search phrase and fulfilling the selection standards, other processes start as follow and mentioned in figure 2. It includes i) Primary Examination Stage: research article is searched using the string or phrases defined earlier in sources like IEEE and Springer. ii) Inferior Examination Stage involves the selection on behalf of research question.

TABLE 2: RESEARCH ARTICLES EVALUATION

Research Articles	Rank	Points	Quality Evaluation
MES V-II [9]	2	1.5	Decent
DSKM [10]	0	0	Low
CBC-RC5 [11]	2	1.5	Decent
HCCTPWLCM [12]	2	1.5	Decent
ECCGASONeC[3]	3	2	Outstanding
QTL [13]	2	1.5	Decent
UES-IV [14]	2	1.5	Decent
LiCi	2	1.5	Decent
LCSA [15]	2	1.5	Decent
ESDCBE [16]	2	1.5	Decent
Multiplexing AES [17]	2	1.5	Decent
AES-QPSK [18]	2	1.5	Decent
ECC-DA[19]	2	1.5	Decent
EEM [20]	2	1.5	Decent
LPRGA [21]	2	1.5	Decent
LED [22]	2	1.5	Decent
SECM [23]	3	2	Outstanding
DCA-SNC[24]	2	1.5	Decent
ECC-KM [25]	1	1	Average
ECB[26]	2	1.5	Decent
MR_XOR [27]	2	1.5	Decent
CP-ABE [28]	2	1.5	Decent
ECC-AES [29]	2	1.5	Decent
MutationAES[30]	2	1.5	Decent
RSA approach [31]	2	1.5	Decent
MRSA [27]	2	1.5	Decent
Chaos-based [32]	3	2	Outstanding
HE [33]	2	1.5	Decent
RSA, ECDH-KE [34]	2	1.5	Decent

AES with HECC [4]	3	2	Outstanding
XOR using Logistic and Kent maps[6]	2	1.5	Decent
Homomorphic data encryption [35]	2	1.5	Decent
DNA-ECC [5]	2	1.5	Decent
E-AES [79]	2	1.5	Decent
RC5-Chaotic Map [80]	2	1.5	Decent

II. Literature Review

Data confidentiality is a complex problem for WSN. A key challenge is to propose a security algorithm which, considering the challenges of low power, coverage problems and limited bandwidth, secures the details.Several components have been extended into research studies of algorithms utilising fewer tools, including elliptical curve, AES, RSA, chaotic maps, efficient block cyphers, and numerous other techniques. There are many protected data methods, but the cryptographic approach is the most common approach where security is considered. Multiple cryptographic approaches are studied to check which methods reduce sensors lifetime. Any algorithm, which has high number of steps, will have high computational cost that reduces the sensor lifetime.

A. ECC based Security Approaches in WSN

Elliptic Curve Cryptography (ECC)[3] is a modern Elliptic Curve key generation system. For the encryption and decryption of data with a key size of 176 bits, the Genetic Algorithm approach is used. A unique key is generated using ECC, where node ID and distance to CH (Cluster Head) are both considered. The main is separated into two components that are XORed with the plaintext. The text is then mutated in order to develop a rare, unreadable cipher-text. To determine the efficient path, genetic algorithm routing is used for the data. This strategy is covered in terms of vulnerability analysis against passive attacks, main space analysis attacks, corrupted CH attacks, Sinkhole attacks, HELLO floods and DOS (Denial of Service) attacks. When using ECC, this technique can suffer from brute-force attacks [36]. By using the method, the use of the Pseudo Random Number Generator (PRNG) in [10] can be violated. Cryptography of the Elliptic Curve-Dynamic Paradigm (ECC-DA) is a cryptographic method that uses elliptic curves to produce keys. For the encryption method that is specified in [19], these produced keys are used. The obtained results of this method devour less time and memory. This algorithm also uses hashing in order to secure data.

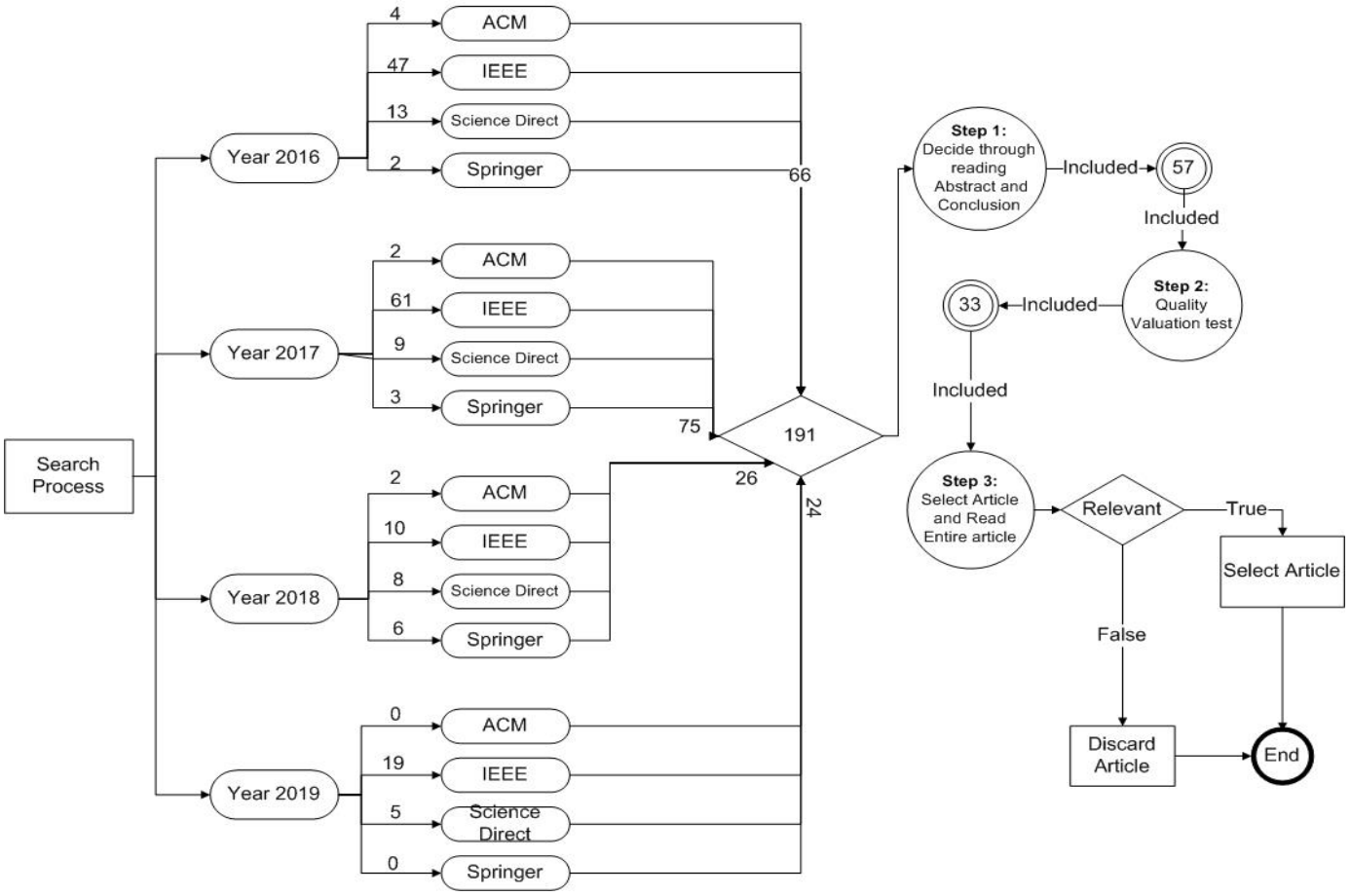

Fig. 2. Article Selection Process

The use of ECC may make it vulnerable to brute attack [37]. In this analysis, the use of hash features renders it vulnerable to slide attacks [38]. PRNG renders this algorithm unprotected against direct cryptanalytic attacks, input-based attacks, meet-in-the-middle attacks and several others [39].

Stable encryption is introduced in this analysis [23]. It utilises the ECC, disorderly map, and genetic algorithm. For data encryption, the procedure uses XOR, mutation and crossover operations. Parameters are calculated in terms of the network's throughput, transmission rate, and lifespan. In terms of all dimensions, this approach provides improved results. This technique of study is protected against a routing threat. This algorithm only uses XOR for encryption in terms of protection, rendering it insecure against known plaintext and chosen plaintext attacks [40]. Elliptic Curve Cryptography-Key Management (ECC-KM)[25] provides a key management approach for stable key generation using ECC, ECC community rules, and ECC discrete logarithmic. The technique limits the use of positive 256-bit integers where each of the private and public keys is both 256 bits. The technique against collision scan attacks is insecure [41]. Hybrid Elliptic Curve Cryptography (HECC) [4] uses a hybrid key generation technique for encryption/decryption and node authentication. Recent studies have shown that it is vulnerable to invalid ECC curve attacks [42]. Setup, Session Key Generation, Node Authentication, Secure Data Exchange, and Key Update [4] are divided into five levels. The technique provides authentication, replay confidentiality, man-in-the-middle, masquerading and attacking eavesdropping. In addition, the random number generator [43] is fragmented. AES is used in this strategy to provide data protection, making this system vulnerable to bicycle attacks [44]. For data encryption and decryption, ECC and DNA [5] are used. To grant genes that are used for data encryption, DNA is used. The result is derived based on the execution time needed for various data sizes for DNA-based encryption. This approach shows that under given conditions, StDT15 (Steroid dehydrogenase) performs betterIt shows that when energy use is measured and calculated, the performance of DNA mapping and encryption is high. It is secure from the SPA's scheduling and threats. This technique is however, vulnerable to man-in-the-middle assault [45]. Regarding an overview of the schemes, ECCGASONeC[3] is known to be better than other ECC methods due to the lower key size and performs better than many current algorithms, including TinyPED and Biswas.Article [81] gives a new data security approach using ECC for key generation. This proposed approach provide security for the node-to-node communication network and hoards memory space on nodes using Elliptic Curve Digital Signature (ECDSA) cryptographic scheme. This research claims to evaluate in terms of key generation time and data packet size. The article [82] discuss new approach, which is similar to ECC. This scheme claims to provide secure key and data transmission between nodes.

B. RSA based Security in WSN

Dual Cryptography Architecture-Secure Network Communication (DCA-SNC) [24] focus on secures data transmission using DNA genes sequence for encryption along with RSA (Rivest, Shamir and Adleman) and DES, however, requires massive amounts of memory and resources. The results present the execution time taken for the generation of SHA functions, DES cypher and RSA key. This methodology is compared with existing RSA and DES, the outcome is that this approach performs better in terms of response time, security, scalability, and practicability. RSA [46], is vulnerable to many attacks. A security concern could be the use of limited public and private key sizes [47]. The study in[31] uses RSA, which is split into four stages: Key Distribution and Generation Stage, Encryption Stage, Enroute Filtering Stage and Routing Stage.2 This proposed methodology evaluated the outcomes of the parameters: production, delivery of packets and consumption of resources. The findings show that this new solution is stronger than the current BECAN algorithm. The RSA in this algorithm makes it vulnerable to attacks by Wiener and Boneh-Durfee[48]. Another encryption method is Modified Rivest-Shamir-Adleman (MRSA), which modifies the current RSA[27] with a key size of 128 bits to 1024 bits. Rather than two prime numbers, this method uses three prime numbers. Three primary numbers help to improve the difficulty of the brute force attack.. On the basis of using various key sizes, outcomes are compared with current RSA, when estimating the overall time it takes for MRSA encryption decryption to make it impossible for brute force attacks to occur. This research methodology is unsafe against a cypher text attack [49]. In addition, due to three prime numbers, energy consumption also increases. To ensure end-to-end security, authentication and convergence, RSA and ECDH-KE (Elliptic-curve Diffie-Hellman-Key Extraction)[50] are used. The Paillier public-key encryption is used by this suggested algorithm by considering other parameters such as stability, energy consumption, computation, and cost of communication. This algorithm provides stronger encryption, authentication, honesty, and privacy in terms of protection. The use of RSA, however, renders this method susceptible to the selected ciphertext attack[49]. ECDH makes man-in-the-middle attacks vulnerable[51]. MRSA[27] is known to be the most successful strategy in terms of protection in all the current literature reviewed on RSA. In addition, it uses limited key sizes varying from 128 bits to 1024 bits that are varied according to specifications for security power. The complex key generation helps in making the data unbreakable. Research article in [83], introduces a new approach NFC with use of key generation through RSA approach. NFC is used in smart phones to open multiple limitless opportunities.

C. Advanced Encryption Standard Security Methods in WSN

Another research approach that uses ECC to produce one encryption key and another decryption key is the ECC-AES (Elliptic Curve Cryptography-Advance Encryption Standard) research approach. [29]. The combination of AES and ECC with a key size of 256 bits offers a highly safe and efficient technique. This algorithm is very safe, but has a high degree of difficulty and a significant overhead for communication [4]. where all the steps of AES are originally done by using multiplexing to combine data [17]. Modified AES uses less resources but offers high security with a 128-bit security key size. AES, however, is vulnerable to biclque attacks [44], a variant of man-in-the-middle attack. The key is also vulnerable to the linked key attack[52]. Another research technique that uses AES [18] is AES-QPSK (Advance Encryption Standard-Quadrature Phase Shift Keying) without and with LDPC (Low-Density Parity Check). Key sizes range from 56, 80, 112, 128- and 256-bit keys. Multiple parameters such as BER (Bit Error Rate) and SNRR are compared to AES with and without LDPC (Signal to Noise Ratio). The result confirms that in the Gaussian channel and fading channel, AES with LDPC is stronger. As there is no key renewal process, the key used in the method will influence the whole technique [26]. It is likely that this technique is not safeguarded against attacks of biclques[44]. This strategy is also vulnerable to main attacks associated with it[52].

AES[20], with a combination of mutation techniques, is used to encrypt files. This approach also uses the combination of AES, primary mutation, seed generation and even and odd mutation. Several attacks, including plaintext, chosen plaintext, chosen cypher text, chosen text, brute force, and cypher text only attacks, are covered by this form. This approach has no defence against differential attacks due to the use of the mutation technique[53] For generation of factors and initial seed, mutation with AES[30] is used. Initial seeds and factors are used to produce the key. This technique is shielded from attacks by mathematical, linear, differential, and brute force. Biclque attacks[44] are particularly insecure. Because of PNRG, direct cryptanalytic attack, input-based attack, backtracking attack and many more are vulnerable[39]. PRNG can be broken down by using the [43] form. Since AES itself is a very complicated approach and requires a significant amount of resources, WSN has learned few AES approaches for data protection due to its smaller key size and less complicated algorithm, AES multiplexing[17] is considered to be more acceptable.

A hybrid approach is used in science [79]. In order to encrypt plaintext blocks, this algorithm uses advanced encryption standard (AES) and elliptic curve encryption (ECC) algorithms and then to get cypher text blocks, using data compression technologies. It then links the ECC-encrypted MAC address and AES key to form a full ciphertext message. The author of this report, after using this method, claims to reduce the time of encryption and improve security. While encryption is reduced, AES and ECC are used for encryption. The sensor will minimise the lifespan of the sensors, which can lead to dead sensor nodes and issues with connectivity.

D. Chaotic Maps Security Methods in WSN

HCCTPWLCM (Hybrid Chaotic Cryptosystem Tent Piecewise Linear Chaotic Map) is a new key management analysis approach that uses chaotic skew and logistic maps[54] with a key scale of 216. The unique key generated is then XORed with the plaintext. In terms of the frequency measure, binary derivation, linear and sequence complexity, RC5 is compared to this approach. As opposed to predecessors, this research methodology provides better results. This algorithm is vulnerable to a selected plaintext attack[55] by Skew map. In terms of security, this method is vulnerable to selected and established plaintext attacks[40] since only XOR operations are used. Another method for protecting data in WSN[16] is Improved Protected Data using Chaotic-Based Encryption (ESDCBE).. For the generation of keys, this strategy uses disorderly maps. The data is then encrypted using the token. Compared to the skipjack algorithm, end-to-end message delay, energy consumption, data and node memory requirements are compared. It does better than skipjack with this algorithm. Chaotic maps can definitely yield unique numbers, but the use of chaotic maps only renders this approach unsafe against ciphertext, known plaintext, selected plaintext and selected ciphertext[56].

For data routing, the LEACH protocol[32] is used and messy maps for data encryption and decryption are used. This approach uses two types of chaotic maps: logistic maps and Lorenz maps The findings equate the LEACH protocol and the testing approach suggested in terms of network lifetime, latency, distribution of packets, and overall consumption of energy. This algorithm worked better than the protocol for LEACH.. It is possible to subdivide unstable maps [57]. Logistic and Kent chaotic maps [6] are used where scheme is split into five parts. The actual image is read in the first section and an original data matrix with a main size of 1060. is created. In the latter step, The initial parameters are used to construct a one-dimensional chaotic logistic sequence. The Kent one-dimensional chaotic sequence is generated using the third step. The created logistic sequence and Kent are combined as a matrix in the fourth Process XORs the generated matrix with the original image matrix in the last step, resulting in an unreadable matrix of ciphertext. There are several drawbacks to this approach, including weak keys, fixed chaotic submatrices Insensitivity to plain images [7]. HCCTPWLCM[12] can be considered to achieve the most favourable results based on studies on data protection using Chaotic Map. This method uses 216 key sizes at most, which is the smallest key size of all Chaotic Map approaches.

E. Lightweight Block Cipher Security Methods in WSN

QTL (A Lightweight Block Cipher) is an ultra-lightweight solution to block cipher[13] with 64 and 128 bit key sizes. S-Boxes for data encryption are used in this technique, where several S-Boxes are created to protect the data.

Main implementation is not designed separately, which helps this system function in an integrated way. To render data stable, the XOR approach is also used. Compared with Piccolo, PRSENT, MIBS and QTL, this approach results in faster work. This strategy is secure from linear differentials. Brute power, algebraic and related-key threats. This strategy, however, is not covered by differential and linear attacks[58]. Another ultra-lightweight block cypher strategy[59] of key size is 128 bits of LiCi. Where plaintext is first split into two data sets, the first set is used for the unreadable generation of data for the S-box. With the first unreadable data generated, the second half of the data is XORed. Then the output is moved three times to the left; the input is then XORed with the first S-box data. This performance is then seven times moved to the left. The final performance is a half-bit criss-cross [5]. Against this strategy, multiple attacks such as linear, discrete, zero correlation and bilique attacks can not be initiated. The algorithm is unsafe against a known and selected plaintext attack[60].

A new LPRGA (Lightweight Pseudo-Random Number Generator) lightweight algorithm was implemented in this study[21]. A secure key and data encryption using RC4 (Rivest Cipher 4) will be enforced. The key is generated at random, and for data encryption, LPRGA is then used. In terms of the randomness test, structural test, time measurement test and unpredictability test, the results are compared. This scheme introduces a new updated main system with RC4 If an important part of the maximum set keystream bit is known[61], it makes it possible for the key to be retrieved. It is possible to conduct a known/chosen plaintext attack against this technique[62] with the use of permutation. The [28] scheme implements a lightweight encryption and authentication code creation scheme for CP-ABE (Ciphertext-Policy Attribute-Based Encryption. Keys are generated using the paillier cryptography algorithm, and these keys are then used to generate certificate authentication DSS (Digital Signature Standard). Safe data against eavesdrop attack is data encryption using this algorithm. Differential attacks can result in SHA-3 [63. Timing attacks can be the product of DSS[64]. Multiple techniques of lightweight block cypher were tested. QTL is the strongest of all of the lightweight methods, as it uses less key size and is considered quicker than current approaches such as Piccolo, PRSENT and MIBS.

In terms of stability, the analysis in[80] uses RC5 and chaotic maps. In the proposed algorithm, the classical Feistel network structure is used, as it is a commonly used block encryption structure with low source consumption. Furthermore, the main chaotic map and RC5 are used to generate. Experimental findings indicate that the proposed testing methodology delivers greater value in terms of security and reliability than current algorithms. Using the messy map and RC5, however, results in high difficulty, which may be a downside to this strategy

F. More Security Techniques in WSN

Several current cryptographic methods are merged under the Ultra-Encryption Protocol Version 4 (UES-IV) Scheme[14] on plaintext, bit-wise reshuffling is performed; then, for unreadable text, bitwise columnar transport is performed. Because multiple encryptions are carried out, it becomes very difficult for brute force attack to predict plaintext. This strategy is not protected from text-only cypher attacks[65. The Low Complexity Protection Algorithm (LCSA)[66] approach requires node creation, the first step in which XOR with plaintext is the key. For data encryption, this technique chooses nodes arbitrarily. N is used as the number of nodes, while node selection is carried out from one to N/2 or N/4 Rather than trying to encrypt every single node, this approach chooses nodes randomly, thereby saving resources. Since nodes are XORed only, they take less time to compute. XOR has a poor defence against attacks by brute force [67]. MR-XOR (Modified Rotation XOR), which is a modified variant of basic XOR[68], is introduced in this scheme. The idea of splitting plaintext and then moving it either to the right or left is used for this algorithm. The data is then XORed with the key, which is predefined, until this stage is finished. In terms of overall throughput and total power overhead, the results are compared. PRNG renders this algorithm vulnerable to a direct cryptanalysis attack, an input-based attack, a meeting-in-the-middle attack, and a few other attacks[39].. The operation of XOR is susceptible to attack by brute force[67][69]. In [35], the algorithm is split into 5 stages, with different functionalities in each step. In this technique, spoofing replay routing information, selective forward, sinkhole, Sybil and HELLO attacks do not occur. In terms of the increasing number of nodes, the effects of the algorithm are contrasted with logistic chaotic and non-linear chaotic systems. It shows that the algorithm works better than counterparts do. Chaotic map makes this algorithm apprehensive from chosen ciphertext and known plaintext attack [70,86-90].

Modern Encryption Standard- Version 4 (MES-IV) [9] is proposed that uses TTJSA (Trisha, Tomodep, Jayshree, Shayan and Asoke) and DJSA (Dripto, Jayshree, Soumirta, Suvadeep, Asoke) for the key generation with variable key size [9]. Encryptions is performed with combination of vernam cipher and CFB (Cipher Feedback Block). It is secure against known plaintext, brute force, differential attack and side channel attacks [71]. In Digital Signature based on Key Management (DSKM) for the data security with small key size [10], SHA-1 is used for public and private keys. Sender uses private key for DS verification message (encryption) and another key is used for decryption. After successful signature verification, message is received, otherwise the message is discarded. SHA-1 makes this approach vulnerable to related-key attack [72]. Asymmetric approach doubles the computation time [73]. In Cipher Channing Block-Rivest Cipher 5 (CBC-RC5) technique, it uses PRNG for randomized key generation [11]. The key is used with CBC-RC5 that acts as a part of block in Cipher Channing Block. Its comparison with SPIN algorithm shows that this methodology is better in terms of network lifetime, time consumption. RC5 weakens it against differential and linear attacks [74]. Moreover, PRNG

has weak defence against from direct cryptanalytic attack, input-based attack, backtracking attack [39].

Honey Encryption (HE) algorithm [33] creates confusion for the attackers. The main idea behind honey encryption is DTE (Distribution Transformation Encodes) [33]. This planned procedure is compared with DPBSV (Dynamic Prime Number Based Security Verification) and AES in terms of control consumption and data travel speed. HE algorithm performs better in terms of both parameters. This technique is secured against brute force attack. This new algorithm uses hash function making the whole algorithm vulnerable to Wagner's generalized attack [75]. A key recovery attack on this cipher can easily be launched [76]. Additional work introduces new approach, which uses Electronic Cipher Block (ECB) for data encryption. A key is generated randomly using PRNG and then combined with ECB for encryption and decryption[26]. The results are paralleled with Diffie-Hellman-Modified Elliptic Curve Cryptography (DH-MECC) in terms of key generation ratio. The results of this technique are better than DH-MECCs in terms of security. The technique has a weak defence against Bleichenbacher's and chosen-plaintext only attacks [77]. Blowfish algorithm in [84] is claimed to be more powerful than ECC and AES. It takes less computational time. In order to verify the originality of data, MD5 algorithm is implemented and to authenticate the client modified Kerberos protocol is applied [91-97]. A new security approach [85] uses modified Diffie-Hellman approach for key generation. This research is designed in term to maintain high-level security yet maintain low computational and response time.

III. Security Analysis:

Based on research in past recent years, it is considered that the entire scheme can be analysed on the prospective of security. In table 3, we have identified that researchers have presented data security in conjunction with routing protocols in one scheme. We have discussed about multiple attacks that have been prevented using various approaches but still suffer from other different attack possibilities and disadvantages. Security analysis of the literature is given in table 4 where attack prevention mechanism is included along with the criticism on these solutions. Several researchers that have either cited these schemes in their research work or compared to present improvements in results identify these critical points. We have identified such schemes and presented a good collection to attract the researchers to propose novel solutions for mitigating the identified attack scenarios. We have evaluated that in [4], it uses AES for encryption of the data, and keys are generated through HECC. The given approach ensures forward and backward secrecy. However, this approach can be compromised by exploiting its random number generator. The use of AES makes this approach vulnerable to biclques attacks. Another approach in [27] modifies the RSA where three prime numbers are used instead of two, which make brute force attack difficult to occur. The use of RSA however makes this approach insecure to chosen ciphertext attack. We have identified that ECCGASONeC [3] presents a routing and a security protocol which helps in both the security of the data and less energy consumption. As per the demand of WSN, this algorithm consumes less energy and secures data. On the contrary, if only high level security is the major concern, AES with HECC [4] is the ideal approach. After examining article from previous years, few techniques are compared in terms of computational time. The approaches where the ciphertext size increase significantly may result in overhead. ECCGASONeC [3] and SEEA [85] works better to provide security with less computations.

Table 3: Co-occurrence of Data Security and Routing in Schemes

Reference	Data Security	Routing	Comments
MES V-II [9]	✓	×	– Gives secure key
DSKM [10]	×	×	– Reduce energy
CBC-RC5 [11]	✓	×	– Proves being better than SPIN algorithm
HCCTPWLCM [12]	✓	×	– Better than RC5
ECCGASONeC[3]	✓	✓	– Less key and plaintext size
QTL [13]	✓	×	– Faster than Picolo, PRESENT, MIBS
UES-IV [14]	✓	×	Unbreakable Data security
LiCi	✓	×	– Less memory consumption
LCSA [15]	✓	×	– Less time consuming
ESDCBE [16]	✓	×	– Better performance than skipjack
Multiplexing AES [17]	✓	×	– Improved AES version for WSN
AES-QPSK [18]	✓	×	– AES with LDPC gives better performance
ECC-DA[19]	✓	×	– Less computational time yet very secure data algorithm
EEM [20]	✓	×	– Less computational time
LPRGA [21]	✓	×	– Better key selection
LED [22]	✓	×	– Better than AES in terms of maintain less computational time
SECM [23]	✓	✓	– Less throughput and delivery rate
DCA-SNC[24]	✓	×	– Better response time, security and scalability
ECC-KM [25]		✓	– Better ECC results
ECB(public key)[26]	✓	×	– Time consumption is high
MR_XOR [27]	✓	×	– Better throughput and total overhead rate
CP-ABE [28]	✓	×	– Lightweight encryption
ECC-AES [29]	✓	×	– Very secure and efficient

MutationAES[30]	✓	×	–	Less energy consumption
RSA approach [31]	✓	×	–	Performance is better than BECAN
MRSA [27]	✓	×	–	High security than RSA
Chaos-based [32]	✓	✓	–	Healthier than LEACH in terms of lifetime, throughput, packet delivery, and total energy
HE [33]	✓	×	–	Better than DPBSV and AES
RSA and ECDH-KE [34]	✓	×	–	Less energy consumption, and communication cost
AES with HECC [4]	✓	✓	–	Less computational cost
XOR using Logistic & Kent maps[6]	✓	×	–	Better performance
Chaotic data integrity & homomorphic encrypt [35]	✓	×	–	Performance is better than MD5
DNA-ECC [5]	✓	×	–	Secure data encryption algorithm
E-AES [79]	✓	×	–	Secure encryption algorithm yet less encryption time consumption.
RC5-Chaotic Map [80]	✓	×	–	Secure data encryption algorithm

TABLE 4: SECURITY ANALYSIS FOR ATTACK PREVENTION AND ATTACK POSSIBILITY IN SCHEMES

Sr	Technique Name	Attack Prevention	Criticism
1	MES V-II [9]	Prevent from known plaintext, brute force and differential attack.	– Side channel attack can occur [71].
2	DSKM [10]	-	– Vulnerable to related-key attacks [72].
3	CBC-RC5 [11]	-	– Differential and linear attacks occur because of RC5 [74]. PNRG causes direct cryptanalytic, input-based and backtracking attacks [39]
4	HCCTPWLCM [12]	-	– Chosen plaintext attack can occur due to XOR. Also suffer from known plaintext attack [55][40].
5	ECCGASONeC[3]	Passive attack, key space analysis, compromised CH, Sinkhole, HELLO flood and DOS attacks cannot occur	– vulnerable to brute force attack [36]. The intruder can use the short period of PRNG (Pseudorandom Number Generator) to generate private keys, as this technique allows to generate random number (Key) [43].
6	QTL [13]	Prevent from differential, linear. Algebraic and related-key attacks.	– Even after claiming, the proposed algorithm suffer from differential and linear attacks. [58]
7	UES-IV [14]	Protect against brute-force attack	– Ciphertext-only attack can occur. [65]
8	LiCi	Linear, differential, zero correlation and bilique attacks cannot occur	– Suffer from known plaintext, and chosen plaintext attacks
9	LCSA [15]	-	– Brute force can occur [67] and can also suffer from known plaintext attack [69].
10	ESDCBE [16]	-	– Ciphertext-only, known, chosen plaintext, and chosen ciphertext attacks [56].
11	Multiplexing AES [17]	-	– Because of the usage of AES, therefore biclques [44] and related key attacks can occur [52].
12	AES-QPSK [18]	Without LDPC & QPSK with LDPC	– Can suffer from biclques [44], related key attacks [52].
13	ECC-DA[19]	-	– Due to hash function slide attacks [38] occur, PRNG on ECC, insecure against Direct Cryptanalytic, input based, meet-in-the-middle attack[39].
14	EEM [20]	Known, chosen plaintext & ciphertext, brute force and cipher text only attacks	– High risk of differential attacks [53].
15	LPRGA [21]	-	– Usage of randomly choosing method, known and chosen plaintext attacks can occur [62].
16	LED [22]	Replay, eavesdropping and known-key attacks can occur.	– Because of SHA-1 it can suffer from collision search attacks [78].
17	SECM [23]	-	– XOR causes known and chosen plaintext attack [40].
18	DCA-SNC[24]	Brute-force attack cannot occur	– RSA is attackable [63]. Small public and private key occurrence as given in [64].
19	ECC-KM [25]	-	– ECC collision attack occur [41]. And invalid curve attack can also occurs [42].
20	ECB [26]	-	– Vulnerable to chosen-plaintext attack [77].
21	MR_XOR [27]	-	– PRNG causes direct cryptanalysis attack, input based attack, meet-in-the-middle attack [39]
22	CP-ABE [28]	Eavesdrop does not occur.	– SHA-3 can get effected from differential attack [63].
23	ECC-AES [29]	-	– Security, high complexity and communication [4].
24	MutationAES [30]	statistical, linear, differential and brute force attacks cannot occur	– Biclques attacks can occur in AES, as proved in [44]
25	RSA based approach [31]	Not mentioned	– It uses RSA for security, which risk from serval attack known as Wiener and Boneh-Durfee attacks [48].
26	MRSA [27]	Brute force hard to occur.	– RSA with same basic algorithm, it is vulnerable to chosen ciphertext attack [49].
27	Chaos-based [32]	-	– Logistic and Lorenz maps same as chaotic maps are attackable, or breakable [57].
28	HE [33]	Brute force attack cannot occur, since hash function is used, and random generation of number is used.	– The new algorithm is given using honey encryption, which uses hash function making the whole algorithm at risk Wagner's generalized attack as proved in [75]. – A recovery attack can also occur [76]
29	RSA and ECDH-KE [34]	-	– Uses RSA, which suffers chosen ciphertext attack [49]. ECDH suffers from man-in-the-middle attack [51].
30	AES with HECC [4]	protection against forward-secrecy, and backward secrecy	– Uses RNG that can be regenerated [43]. AES suffers from biclques attacks [44].

31	Logistic and Kent maps [6]	-	- Infeasible for securing medical images. Disadvantages of weak keys, fixed chaotic sub-matrices, and plain-image insensitivity as mentioned in [7].
32	Homomorphic encryption [35]	Stops spoofing, replay, selective forward, sinkhole, Sybil and HELLO	- chaotic map which makes this algorithm suffer from chosen ciphertext and known plaintext attack [70].
33	DNA-ECC [5]	Safe for Timing and SPA attacks.	- Insecure from man-in-the-middle attack [45].
34	E-AES [79]	Uses AES and ECC for security	- Vulnerable to High complexity, and reduce network lifetime
35	RC5-Chaotic Map [80]	Uses RC5 for encryption and Chaotic Map for key generation	- Vulnerable to High complexity, and reduce network lifetime

Figure 3 illustrates a fish diagram to present causes of attacks that can affect data security in WSN. Different approaches are proposed to overcome data security problem in WSN. One-problem remains where proposed methodologies for data security has high computational time resulting into reducing the network lifetime, consuming high energy and takes up large memory space.

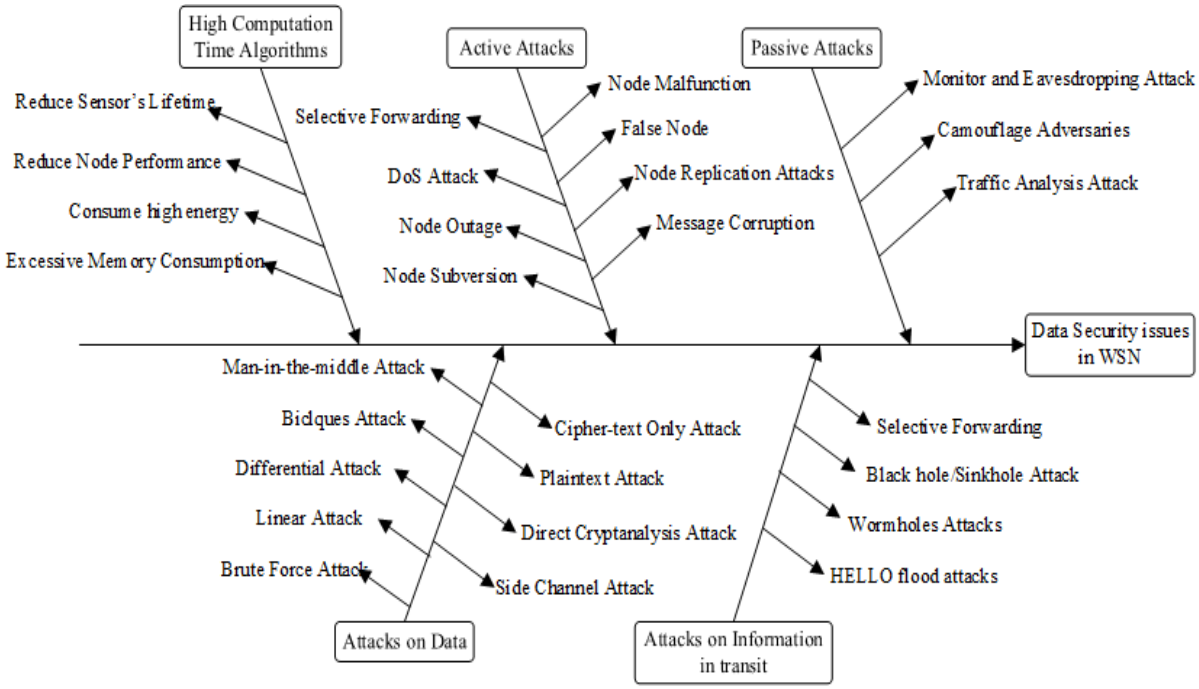

Fig. 3. Cause and Effect Diagram of Data Security in WSN

IV. Conclusion

This survey discusses systematic literature review performed in order to build research question and literature review. SLR steps are performed in order to select articles related to research question as described in section 2. This paper has assembled security fundamental in WSN after the study of multiple articles. Since WSN is an intricate environment, few research approaches are suitable as per selection criteria. Various research methodologies provide high security algorithm, while increasing the complexity and decreasing sensor network lifetime. Other research methodologies provide less complex security approaches but considered as not strongly secure enough. We have selected 31 articles out of 167 after performing SLR. Literature, incudes ECC, AES, RSA, Chaotic maps and efficient block ciphers-based techniques that are evaluated for key and plain text sizes along with other features and results. We have also performed security analysis to identify the discrepancies of schemes that resolve the attack scenarios but still suffer from other attacks. We have also differentiated among schemes that separately provide data security scheme or involve the secure routing protocols as well. Finally, a fish diagram is presented to illustrate the attack scenarios. Wireless sensor network is still not able to handle high computational algorithm, because these types of algorithms reduce network lifetime. We have identified that most of the data security approaches used in WSN are not suitable because of higher computations and slow response. It arises a need for data security approach with less computational time in future.

V. References:

[1] "The Network and Security Analysis for Wireless Sensor Network : A Survey." [Online]. Available: https://www.researchgate.net/publication/283271334_The_Network_and_Security_Analysis_for_Wireless_Sensor_Network_A_Survey. [Accessed: 25-Sep-2020].

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.
[3] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 28, no. 3, pp. 262–275, 2016.
[4] I. Ullah, N. ul Amin, J. Iqbal, M. Shahid, and F. Ali, "An Efficient Secure Protocol for Wireless Sensor Networks Based on Hybrid Approach," *IJCSNS*, vol. 18, no. 6, p. 59, 2018.
[5] H. D. Tiwari and J. H. Kim, "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices," *ETRI J.*, vol. 40, no. 3, pp. 396–409, 2018.
[6] W. Wang *et al.*, "An encryption algorithm based on combined chaos in body area networks," *Comput. Electr. Eng.*, vol. 65, pp. 282–291, 2018.
[7] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. S. Beg, and A. A. Alzaidi, "Cryptanalysis of an Image Encryption Algorithm Based on Combined Chaos for a BAN System, and Improved Scheme Using SHA-512 and Hyperchaos."
[8] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.
[9] A. Praveena and S. Smys, "Efficient cryptographic approach for data security in wireless sensor networks using MES VU," in *Intelligent Systems and Control (ISCO), 2016 10th International Conference on*, 2016, pp. 1–6.
[10] G. J. Shruthi, "Digital signature based key management protocol for secure data transfer in dynamic wireless sensor networks," in *Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on*, 2016, pp. 499–502.
[11] I. J. Habeeb and R. A. Muhajjar, "Secured Wireless Sensor Network Using Improved Key Management," in *Proceedings of the Fifth International Conference on Network, Communication and Computing*, 2016, pp. 302–305.
[12] H. M. Al-Mashhadi, H. B. Abdul-Wahab, and R. F. Hassan, "Data Security Protocol for Wireless Sensor Network using Chaotic Map," *Int. J. Comput. Sci. Inf. Secur.*, vol. 13, no. 8, p. 80, 2015.
[13] L. Li, B. Liu, and H. Wang, "QTL: A new ultra-lightweight block cipher," *Microprocess. Microsyst.*, vol. 45, pp. 45–55, Aug. 2016.
[14] A. Praveena, "Achieving data security in wireless sensor networks using ultra encryption standard version #x2014; IV algorithm," in *2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)*, 2017, pp. 1–5.
[15] A. Rani and S. Kumar, "A low complexity security algorithm for wireless sensor networks," in *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, 2017, pp. 1–5.
[16] C. Bayılmış, Ü. Çavuşoğlu, A. Akgül, S. Kaçar, and A. Sevin, "Enhanced secure data transfer for WSN using chaotic-based encryption," *Teh. Vjesn.*, vol. 24, no. 4, pp. 1065–1069, 2017.
[17] J. Li, "A Symmetric Cryptography Algorithm in Wireless Sensor Network Security," *Int. J. Online Eng. IJOE*, vol. 13, no. 11, pp. 102–110, 2017.
[18] A. Khan, S. W. Shah, A. Ali, and R. Ullah, "Secret key encryption model for Wireless Sensor Networks," in *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*, 2017, pp. 809–815.
[19] S. Som, R. Majumder, and S. Dutta, "Elliptic curve cryptography: A dynamic paradigm," in *Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017 International Conference on*, 2017, pp. 427–431.
[20] A. Vangala and P. Parwekar, "Enhanced encryption model for sensor data in wireless sensor network," in *2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2017, pp. 16–21.
[21] S. Maity, K. Sinha, and B. P. Sinha, "An efficient lightweight stream cipher algorithm for wireless networks," in *Wireless TCommunications and Networking Conference (WCNC), 2017 IEEE*, 2017, pp. 1–6.
[22] K.-L. Tsai, F.-Y. Leu, T.-H. Su, and Y.-C. Chang, "A Light Weight Data Encryption Method for WSN Communication," in *International Conference on Broadband and Wireless Computing, Communication and Applications*, 2017, pp. 788–795.
[23] R. Santhosh and M. Shalini, "Security Enhancement using Chaotic Map and Secure Encryption Transmission for Wireless Sensor Networks."
[24] H. Suresh and R. S. Hegadi, "DCA-SNC: Dual Cryptosystem Architecture for Secure Network Communication," *Int. J.*, vol. 7, no. 1, 2017.
[25] S. R. Singh, A. K. Khan, and T. S. Singh, "A New Key Management Scheme for Wireless Sensor Networks using an Elliptic Curve," *Indian J. Sci. Technol.*, vol. 10, no. 13, 2017.
[26] P. L. K. Reddy, B. R. B. Reddy, and S. R. Krishna, "Secure Random Bit Size Encryption Algorithm for Wireless Sensor Data Transmission," 2018.
[27] D. Roy and P. Das, "A Modified RSA Cryptography Algorithm for Security Enhancement in Vehicular Ad Hoc Networks," in *Proceedings of the International Conference on Computing and Communication Systems*, 2018, pp. 641–653.
[28] M. Solomon and E. P. Elias, "Data Security and Privacy in Wireless Sensor Devices," *networks*, vol. 5, no. 05, 2018.
[29] S. Prakash and A. Rajput, "Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks," in *Ambient Communications and Computer Systems*, Springer, 2018, pp. 589–599.
[30] A. Vangala and P. Parwekar, "Encryption Model for Sensor Data in Wireless Sensor Networks," in *Information Systems Design and Intelligent Applications*, Springer, 2018, pp. 963–970.
[31] B. Sreevidya, M. Rajesh, and T. M. Mamatha, "Design and Development of an Enhanced Security Scheme Using RSA for Preventing False Data Injection in Wireless Sensor Networks," in *Ambient Communications and Computer Systems*, Springer, 2018, pp. 225–236.
[32] M. P. Nidarsh and M. G. P. Devi, "Chaos based Secured Communication in Energy Efficient Wireless Sensor Networks," *Chaos*, vol. 5, no. 06, 2018.
[33] P. L. Gracy and D. Venkatesan, "An Honey Encryption Based Efficient Security Mechanism For Wireless Sensor Networks," *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 3157–3164, 2018.
[34] S. S. Babu and K. Balasubadra, "Revamping data access privacy preservation method against inside attacks in wireless sensor networks," *Clust. Comput.*, pp. 1–11, 2018.
[35] B. Madhuravani, D. S. R. Murthy, and S. V. Raju, "An Improved Wireless Node Neighbor Integrity Verification and Encryption using Additive and Multiplicative Homomorphic Model," *J. Fundam. Appl. Sci.*, vol. 10, no. 6S, pp. 2911–2932, 2018.
[36] K. M. Finnigin, B. E. Mullins, R. A. Raines, and H. B. Potoczny, "Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks," *Int. J. Secur. Netw.*, vol. 2, no. 3–4, pp. 260–271, 2007.
[37] K. Somsuk and C. Sanemueang, "The New Modified Methodology to Solve ECDLP Based on Brute Force Attack," in *International Conference on Computing and Information Technology*, 2018, pp. 255–264.
[38] M. Gorski, S. Lucks, and T. Peyrin, "Slide Attacks on a Class of Hash Functions," 263, 2008.

[39] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic attacks on pseudorandom number generators," in *International Workshop on Fast Software Encryption*, 1998, pp. 168–188.

[40] J. Daemen, "Limitations of the Even-Mansour construction," in *International Conference on the Theory and Application of Cryptology*, 1991, pp. 495–498.

[41] M. J. Wiener and R. J. Zuccherato, "Faster attacks on elliptic curve cryptosystems," in *International workshop on selected areas in cryptography*, 1998, pp. 190–200.

[42] S. Neves and M. Tibouchi, "Degenerate curve attacks: extending invalid curve attacks to Edwards curves and other models," *IET Inf. Secur.*, vol. 12, no. 3, pp. 217–225, 2017.

[43] J. Reeds, "'Cracking' a random number generator," *Cryptologia*, vol. 1, no. 1, pp. 20–26, 1977.

[44] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2011, pp. 344–371.

[45] S. Roy and C. Khatwani, "Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols," *Cryptography*, vol. 1, no. 1, p. 9, 2017.

[46] A. Nitaj, M. R. K. Ariffin, D. I. Nassr, and H. M. Bahig, "New attacks on the RSA cryptosystem," in *International Conference on Cryptology in Africa*, 2014, pp. 178–198.

[47] L. R. Date, "Attacks On the RSA Cryptosystem."

[48] B. De Weger, "Cryptanalysis of RSA with small prime difference," *Appl. Algebra Eng. Commun. Comput.*, vol. 13, no. 1, pp. 17–28, 2002.

[49] J. Manger, "A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS# 1 v2. 0," in *Annual International Cryptology Conference*, 2001, pp. 230–238.

[50] Y. Lindell and J. Katz, *Introduction to modern cryptography*. Chapman and Hall/CRC, 2014.

[51] R. Haakegaard and J. Lang, "The Elliptic Curve Diffie-Hellman (ECDH)," *Online Httpskoclab Cs Ucsb Eduteachingeccproject2015ProjectsHaakegaard Lang Pdf*, 2015.

[52] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full AES-192 and AES-256," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2009, pp. 1–18.

[53] E. M. B. Albassal and A.-M. Wahdan, "Genetic algorithm cryptanalysis of the basic substitution permutation network," in *Circuits and Systems, 2003 IEEE 46th Midwest Symposium on*, 2003, vol. 1, pp. 471–475.

[54] H. M. Al-Mashhadi, H. B. Abdul-Wahab, and R. F. Hassan, "Data Security Protocol for Wireless Sensor Network using Chaotic Map," *Int. J. Comput. Sci. Inf. Secur.*, vol. 13, no. 8, p. 80, 2015.

[55] Y. Chen, X. Liao, and K.-W. Wong, "Chosen plaintext attack on a cryptosystem with discretized skew tent map," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 53, no. 7, pp. 527–529, 2006.

[56] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of dynamic look-up table based chaotic cryptosystems," *Phys. Lett. A*, vol. 326, no. 3–4, pp. 211–218, 2004.

[57] M. I. Sobhy and A.-E. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *icassp*, 2001, pp. 1001–1004.

[58] S. Sadeghi, N. Bagheri, and M. A. Abdelraheem, "Cryptanalysis of reduced QTL block cipher," *Microprocess. Microsyst.*, vol. 52, pp. 34–48, 2017.

[59] J. Patil, G. Bansod, and K. S. Kant, "LiCi: A new ultra-lightweight block cipher," in *2017 International Conference on Emerging Trends Innovation in ICT (ICEI)*, 2017, pp. 40–45.

[60] A. Bogdanov *et al.*, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, 2007, pp. 450–466.

[61] S. Mister and S. E. Tavares, "Cryptanalysis of RC4-like Ciphers," in *International Workshop on Selected Areas in Cryptography*, 1998, pp. 131–143.

[62] S. Li, C. Li, G. Chen, D. Zhang, and N. G. Bourbakis, "A general cryptanalysis of permutation-only multimedia encryption algorithms," *IACR's Cryptol. EPrint Arch. Rep.*, vol. 374, p. 2004, 2004.

[63] Y. Wang and M. Yang, "Higher Order Differential Cryptanalysis on the SHA-3 Cryptographic Hash Algorithm Competition Candidates," 2009.

[64] P. C. Kocher, *Cryptanalysis of di e-hellman, rsa, dss, and other systems using timing attacks*. Manuscript, 1995.

[65] G. Lasry, N. Kopal, and A. Wacker, "Cryptanalysis of columnar transposition cipher with long keys," *Cryptologia*, vol. 40, no. 4, pp. 374–398, 2016.

[66] C. Li, S. Li, G. Alvarez, G. Chen, and K.-T. Lo, "Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations," *Phys. Lett. A*, vol. 369, no. 1–2, pp. 23–30, 2007.

[67] *Simple Brute Force Attack - Google Search*. Accessed: 21-Jul-2018. [Online]. Available: https://www.cloudways.com/blog/what-is-brute-force-attack/

[68] B. AnandaKrishna, N. Madhuri, M. K. Rao, and B. VijaySekar, "Implementation of a novel cryptographic algorithm in Wireless Sensor Networks," in *Signal Processing And Communication Engineering Systems (SPACES), 2018 Conference on*, 2018, pp. 149–153.

[69] *XOR Known-Plaintext Attack | Didier Stevens*. Accessed:21-Jul-2018 [Online]. Available: https://blog.didierstevens.com/2016/01/01/xor-known-plaintext-attack

[70] E. Biham, "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1991, pp. 532–534.

[71] Y. Gao, H. Ao, Z. Feng, W. Zhou, S. Hu, and W. Tang, "Mobile Network Security and Privacy in WSN," *Procedia Comput. Sci.*, vol. 129, pp. 324–330, 2018.

[72] M.-J. O. Saarinen, "Cryptanalysis of block ciphers based on SHA-1 and MD5," in *International Workshop on Fast Software Encryption*, 2003, pp. 36–44.

[73] Y. Kumar, R. Munjal, and H. Sharma, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures," *Int. J. Comput. Sci. Manag. Stud.*, vol. 11, no. 03, 2011.

[74] B. S. Kaliski and Y. L. Yin, "On differential and linear cryptanalysis of the RC5 encryption algorithm," in *Annual International Cryptology Conference*, 1995, pp. 171–184.

[75] J.-S. Coron and A. Joux, "Cryptanalysis of a Provably Secure Cryptographic Hash Function.," *IACR Cryptol. EPrint Arch.*, vol. 2004, p. 13, 2004.

[76] S. Degan, "Cryptanalysis of Hash Functions," 2012.

[77] J.-S. Coron, M. Joye, D. Naccache, and P. Paillier, "New attacks on PKCS# 1 v1. 5 encryption," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2000, pp. 369–381.

[78] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Annual international cryptology conference*, 2005, pp. 17–36.

[79] Yue, T., Wang, C., & Zhu, Z. (2019). Hybrid Encryption Algorithm Based on Wireless Sensor Networks. 2019 IEEE

International Conference on Mechatronics and Automation (ICMA). doi:10.1109/icma.2019.8816451.

[80] Luo, Y., Yao, L., Liu, J., Zhang, D., & Cao, L. (2019). A Block Cryptographic Algorithm for Wireless Sensor Networks Based on Hybrid Chaotic Map. 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/Smart/City/DSS). Doi:10.1109/hpcc/smartcity/dss/2019

[81] Qazi, R., Qureshi, K.N., Bashir, F. et al. Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02020-z

[82] Ravi K., Khanai R., Praveen K. (2020) A Secure Key and Data Exchange Mechanism Using Elliptic Curve Cryptography on WSN. In: Hitendra Sarma T., Sankar V., Shaik R. (eds) Emerging Trends in Electrical, Communications, and Information Technologies. Lecture Notes in Electrical Engineering, vol 569. Springer, Singapore. https://doi.org/10.1007/978-981-13-8942-9_44

[83] P. Satapathy, N. Pandey and S. K. Khatri, "NFC Car Keys By Using RSA Cryptography In WSN Security," 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2019, pp. 143-147, doi: 10.1109/ICECA.2019.8821905.

[84] Neha Gupta & Vivek Kapoor (2020) Hybrid cryptographic technique to secure data in web application, Journal of Discrete Mathematical Sciences and Cryptography, 23:1, 125-135, DOI: 10.1080/09720529.2020.1721872

[85] Ali S, Humaria A, Ramzan MS, et al. An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International Journal of Distributed Sensor Networks. June 2020. doi:10.1177/1550147720925772

[86] Lim, M., Abdullah, A., Jhanjhi, N. Z., Khan, M. K., & Supramaniam, M. (2019). Link prediction in time-evolving criminal network with deep reinforcement learning technique. IEEE Access, 7, 184797-184807.

[88] Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81.

[89] Gaur, L., Singh, G., Solanki, A., Jhanjhi, N. Z., Bhatia, U., Sharma, S., ... & Kim, W. (2021). Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. Human-Centric Computing and Information Sciences, 11, NA.

[90] Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.

[91] Gaur, L., Afaq, A., Solanki, A., Singh, G., Sharma, S., Jhanjhi, N. Z., ... & Le, D. N. (2021). Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. Computers and Electrical Engineering, 95, 107374.

[92] Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In 2018 4th International conference on computer and information sciences (ICCOINS) (pp. 1-5). IEEE.

[93] Adeyemo, V. E., Abdullah, A., JhanJhi, N. Z., Supramaniam, M., & Balogun, A. O. (2019). Ensemble and deep-learning methods

[87] Humayun, M., Ashfaq, F., Jhanjhi, N. Z., & Alsadun, M. K. (2022). Traffic management: Multi-scale vehicle detection in varying weather conditions using yolov4 and spatial pyramid pooling network. Electronics, 11(17), 2748.

for two-class and multi-attack anomaly intrusion detection: an empirical study. International Journal of Advanced Computer Science and Applications, 10(9).

[94] Sennan, S., Somula, R., Luhach, A. K., Deverajan, G. G., Alnumay, W., Jhanjhi, N. Z., ... & Sharma, P. (2021). Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. Transactions on Emerging Telecommunications Technologies, 32(8), e4171.

[95] Alourani, A., Ashfaq, F., Jhanjhi, N. Z., & Ali Khan, N. (2023). BiLSTM-and GNN-Based Spatiotemporal Traffic Flow Forecasting with Correlated Weather Data. Journal of Advanced Transportation, 2023.

[96] Lim, M., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Hidden link prediction in criminal networks using the deep reinforcement learning technique. Computers, 8(1), 8.

[97] Kumar, T., Pandey, B., Mussavi, S. H. A., & Zaman, N. (2015). CTHS based energy efficient thermal aware image ALU design on FPGA. Wireless Personal Communications, 85, 671-696.