WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

A Review of Hash Function Types and their Applications

Hassan F. Al-Layla*, Farah N. Ibraheem and Haifaa Ahmed Hasan

Computer Engineering Department, College of Engineering, University of Mosul

*Corresponding Author: Hassan F. Al-Layla

DOI: https://doi.org/10.31185/wjcm.52

Received: May 2022; Accepted: July 2022; Available online: September 2022

ABSTRACT: In the recent decade, global community has been one of the world's most prominent targets of terrorist strikes. There is still study being done and improved efficiency procedures needed in this sector, however the security forces and law enforcement agencies are creating and launching high security weaponry to secure their territories. There is a huge necessity to include the greater level of protection into military vehicles in the wake of several terrorist attacks and sniffing of security officers. Terrorists rely heavily on infiltration while avoiding detection by security measures because of the holes in these hypothetical situations. This paper presents the central methods of hash functions, cryptography and dynamic encryption that may be utilized by the military personnel to increase the safety, privacy, and resistance to sniffing of their communications with one another. This article details the many methods and algorithms that may be included into laser guided defensive weapons and vehicles to provide safe communication across the system.

Keywords: Cryptography, Defense security, Encryption, Internet of things, IoT, Network security, Wireless security

1. INTRODUCTION

Since its inception in 1880, when A. Graham Bell and C. S. Spoiler patented the photophone, wireless communication has expanded tremendously in terms of invention across many fields. In the early days of wireless technology, it was used for private conversations. Modern wireless innovation accommodates a wide range of frequencies to serve business, consumer, and security needs. For reliable and secure data transfer, wireless networks depend on radio technology and related clustered angles. Many different perspectives on wireless communication exist [1]. Some examples are wireless sensor networks, mobile ad hoc networks, Wi-Max, and many more. Administrators implement cryptography and dynamic encryption to ensure that all communications are secure from eavesdropping and may proceed unhindered [2] [3].

Terrorist attacks of significant size in Iraq are represented by the numbers in Table 1. In order to prevent such situations from happening in the future, it is necessary to identify and resolve their underlying implementations [4].

2. NEED OF HASH FUNCTIONS AND CRYPTOGRAPHY

Vulnerability concerns from a wide variety of sources and channels necessitate extensive study into the vast cryptographic and hashing function-related topic of network security [5].

Through a case study examination of various works by researchers in the field of Internet of Things, this research publication shifts its attention to the network environment (IoT) [6]. Since sensor-based technologies form the backbone of the Internet of Things [7]. integrating security measures into this infrastructure is crucial. Key exchange is pursued using the dynamic cryptography features so that the entire system condition may be created anchored in wireless a system

Table 1. Explain Secured Approaches and Key Aspects.

Feature / Algorithm	Hash	Symmetric	Asymmetric
No. of Keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used	SHA	AES	RSA
Key Management/Sharing	N/A	Big issue	Easy & Secure
Effect of Key compromise	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384 or SHA-512	AES, Blowfish, Serpent, Twofish, 3DES, and RC4	RSA, DSA, ECC, Diffie-Hellman

including advanced scenarios [8]. A thorough review of the manuscript's research, methodology, and cryptography-related concerns for security and honesty in the context of the Internet of Things' wireless situation is under underway [9] [10].

IoT relies on wireless connections between devices, and as a result, it's important to discuss the most effective cryptographic techniques for usage in a wireless setting in order to provide secure, trusted data transfer [11] [12]. This study manuscript proposes using and combining various cryptographic measurements and components with the highly effective quantum cryptography methodologies that are bringing about tremendous distinction and unmistakable quality in the field of information encryption and secured transmission utilizing cryptography [13] [14].

3. KEY APPLICATIONS OF HASH FUNCTIONS AND KEY CRYPTOGRAPHY ASPECTS

To authenticate that we, and not an imposter, signed a paper document, we can use either a digital signature or a handwritten one. This is demonstrated by comparing the current signature with one or more previous signatures [15].

If there is a match, the receiver can safely accept the files without worrying that they were sponsored by an unauthorized third party [16]. If this is the first time, it is likely that they will need to produce some kind of identification and be present in person to sign the necessary paper work [17].

In order to ensure that a file hasn't been tampered with in any way, hash functions are commonly utilized [18]. ZIf you've ever downloaded a free app from the web, you could have looked up the checksum of the file right next to the link to the app's binary executable or archived source code [19].

The software checksum is a crucial piece of information for verifying the authenticity of downloaded programmers [20]. A password is a discrete string of characters used to unlock data, software, or an entire machine. Password is an archaic term that has been in use for quite some time. Soldiers stationed to keep watch over a building could recognize a secret term or phrase exchanged between friends [21].

Key Derivation Key derivation is the process of creating several keys for cryptographically securing a connection session from a single secret password or passphrase that is communicated between two parties [22].

For instance, two people can work together to generate encryption and authentication keys by agreeing on a secret key and then passing that key to a key derivation algorithm. To put it another way, even if an attacker has the authentication key, they will be unable to decrypt the data [23]. It is preferable to link a time with a record so as to attest to the record's actual existence at that moment, and this is where digital time stamping comes in. When two or more people are arguing about who was the first to make a discovery or develop something, time-stamping can be a crucial factor in settling the argument [24].

Rootkit Detection Hackers often install software on a victim's computer called "root kits" to hide the attempts of other malicious software to compromise the system's underlying operating system [25]. A Rootkit hides its existence on a compromised machine. Signature-based discovery is one way for spotting rootkits; it entails using scanning tools, such antivirus or antispyware, to look for traces of recognized rootkit signatures on the system [26].

Table 2. Evaluation of Research Manuscripts in Literature

Manuscript	Advantages	Limitations
1	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Lacking in Generalization
2	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors

Continued on next page

Table 2 continued

3	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
4	Assorted Parameters for Cumulative Security and Integrity	Overall Implementation Patterns
5	Higher Degree of Security and Anti-Hacking Mechanisms	Complexity and Trade-Off Factors
6	Assorted Parameters for Cumulative Security and Integrity	Overall Implementation Patterns
7	Higher Degree of Security and Anti-Hacking Mechanisms	Complexity and Trade-Off Factors
8	Assorted Parameters for Cumulative Security and Integrity	Implementation for Diverse Applications
9	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
10	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Lacking in Generalization
11	Cumulative Integrity, Security and Privacy	Implementation for Diverse Applications
12	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
13	Higher Degree of Security and Anti-Hacking Mechanisms	Implementation for Diverse Applications
14	Cumulative Integrity, Security and Privacy	Lacking in Generalization
15	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors
16	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors
17	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
18	Higher Degree of Security and Anti-Hacking Mechanisms	Implementation for Diverse Applications
19	Assorted Parameters for Cumulative Security and Integrity	Implementation for Diverse Applications
20	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors
21	Cumulative Integrity, Security and Privacy	Implementation for Diverse Applications
22	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Complexity and Trade-Off Factors
23	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
24	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
25	Higher Degree of Security and Anti-Hacking Mechanisms	Lacking in Generalization
26	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors
27	Assorted Parameters for Cumulative Security and Integrity	Complexity and Trade-Off Factors
28	Assorted Parameters for Cumulative Security and Integrity	Complexity and Trade-Off Factors
29	Multi-Dimensional Performance, Evaluation Patterns, Effectiveness	Implementation for Diverse Applications
30	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors
31	Cumulative Integrity, Security and Privacy	Implementation for Diverse Applications
32	Cumulative Integrity, Security and Privacy	Complexity and Trade-Off Factors
33	Cumulative Integrity, Security and Privacy	Lacking in Generalization
34	Higher Degree of Security and Anti-Hacking Mechanisms	Complexity and Trade-Off Factors

Continued on next page

Table 2 continued

35	Higher Degree of Security and Anti-Hacking Mechanisms	Complexity and Trade-Off Factors
36	Assorted Parameters for Cumulative Security and Integrity	Overall Implementation Patterns
37	Assorted Parameters for Cumulative Security and Integrity	Overall Implementation Patterns
38	Assorted Parameters for Cumulative Security and Integrity	Lacking in Generalization
39	Higher Degree of Security and Anti-Hacking Mechanisms	Implementation for Diverse Applications
40	Assorted Parameters for Cumulative Security and Integrity	Lacking in Generalization
41	Cumulative Integrity, Security and Privacy	Implementation for Diverse Applications
42	Higher Degree of Security and Anti-Hacking Mechanisms	Lacking in Generalization

4. PERSPECTIVES ON CRYPTOGRAPHY AND RELATED AREAS:

The term "cryptography" is used to refer to the creation and use of methods and procedures that provide secure communication through predetermined channels [27]. It has long been associated with encryption techniques for handling transmission security. The use of cryptographic tools, such as encryption and message confirmation schemes, can help achieve security goals [28].

Secret-Key Encryption with an Asymmetric Parameter (or Public Key Cryptography) I Table 5. Asymmetric key cryptography relies on the use of mathematical formulations and functions that pair together distinct keys. In addition, the associated mathematical fuzzy functions are completed. Numerous asymmetric key cryptographic methods exist, but one of the most popular is RSA-based encryption [29].

A Brief Introduction to the RSA Algorithm Figure 1 Illustrated this

- The RSA initials stand for Rivest, Shamir, and Adelman, the creators of this particular algorithm.
  This means that if one key is made public, the other must be kept secret, and vice versa.
- You may choose between a 512-bit, 1024-bit, or 2048-bit key.

The many cryptographic methods may be broken down into the following categories:

Based on the Security by Obscurity Approach, the whole cryptosystem is communicating securely while maintaining a high level of privacy. In contrast, modern cryptography makes use of data science and mathematical functions, as well as binary operations and bit-wise manipulations, and incorporates a secret key.

Steganography is another method for protecting sensitive data in large-scale operations [30] [31]. The main distinctions between cryptography and Steganography are as follows.

The many cryptographic methods may be broken down into the following categories:

Based on the Security by Obscurity Approach, the whole cryptosystem is communicating securely while maintaining a high level of privacy. In contrast, modern cryptography makes use of data science and mathematical functions, as well as binary operations and bit-wise manipulations, and incorporates a secret key.

Steganography is another method for protecting sensitive data in large-scale operations [30] [31]. The main distinctions between cryptography and Steganography are as follows.

Table 3 and 4 detail thevarious cryptographic methods and their associated assessment criteria, allowing for vast analytical exploration.

5. OPEN-SOURCE CRYPTOGRAPHY LIBRARIES FOR RESEARCH

- NaCL
- Bouncy Castle
- cryptlib
- GnuTLS

Table 3. **Explain Secret-Key Encryption with an Asymmetric Parameter (or Public Key Cryptography)**

Algorithm	The Size of the Message Digest (bit)	Message Block Size	Collision
MD2	128	128	Yes
MD4	128	512	Almost
MD5	128	512	Yes
RIPEMD	128	512	Yes
RIPEMD-128/256	128/256	512	No
RIPEMD-160/320	160/320	512	No
SHA-0	160	512	Yes
SHA-1	160	512	There is a Disability
SHA-256/224	256/224	512	No
SHA-512/384	512/384	1024	No
WHIRPOOL	512	512	No

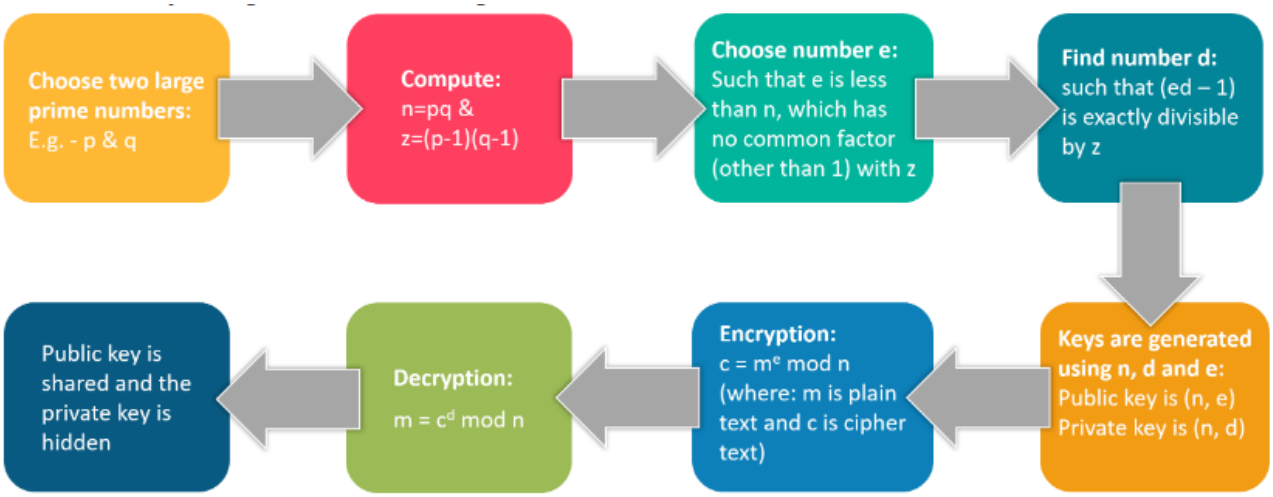

FIGURE 1. **RSA based Encryption.**

Table 4. **Comparison of Cryptography and Steganography**

KEY POINT	STEGANOGRAPHY	CRYPTOGRAPHY
Supported security principles	Authentication, Confidentiality	Data integrity, Confidentiality, authentication, and non-repudiation.
Goal	Communication	Data protection and Security
Techniques	Transform domain, Spatial domain, model-based and ad-hoc.	Substitution, Transposition, block ciphers, stream cipher
Structure of the message	Not altered	Transmission based
Basic	Cover writing with multimedia	Encryption
Popularity	Not Frequent	Widely used
Types of attack	Steg-analysis	Cryptanalysis
Relies on	Key	Not specific parameters
Implementation	Multimedia	Text File

Table 5. Symmetric and Public Key Cryptosystems

	Public Key Cryptosystems	Symmetric Cryptosystems
Association in Keys	Different, but mathematically related	Same
Decryption Key	Private	Symmetric
Encryption Key	Public	Symmetric

- libsodium
- Libgcrypt
- OpenSSL
- Network Security Services (NSS)
- Crypto++
- Nettle
- Botan
- wolfCrypt

Table 6. Comparative Evaluation of Key generation and exchange

Implementation	DH	ECDH	DSA	RSA	ElGamal	NTRU	DSS
Botan	Yes	Yes	Yes	Yes	Yes	No	Yes
Bouncy Castle	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Crypto++	Yes	Yes	Yes	Yes	Yes	No	Yes
Libgcrypt	Yes	Yes	Yes	Yes	Yes	No	Yes
Libsodium	Yes	No	Yes	No	No	No	No
Nettle	No	No	Yes	Yes	No	No	No
Cryptlib	Yes	Yes	Yes	Yes	Yes	No	Yes
OpenSSL	Yes	Yes	Yes	Yes	No	No	No
wolfCrypt	Yes	Yes	Yes	Yes	No	Yes	Yes

The segment summarizes the cryptography-based methods, including their essential characteristics and the availability of particular secured implementations, over a range of relevant parameters. In the table 5, a "1" indicates the presence of the specified trait, while a "0" indicates its absence, in Figure 2: Explain Open-Source Cryptography.

Here many popular implementations of public key cryptography with their respective standards in Table 6, all of which have shown to be highly effective in the aggregate across a variety of use cases.

Table 7. Public key cryptography standards in the Cryptography Implementations

Implementation	PKCS#Yes	PKCS#5	PKCS#8	PKCS#Yes2	IEEE PYes363	ASN.Yes
Botan	Yes	Yes	Yes	No	Yes	Yes
Bouncy Castle	Yes	Yes	Yes	Yes	Yes	Yes
Cryptlib	Yes	Yes	Yes	Yes	No	Yes
Crypto++	Yes	Yes	Yes	No	Yes	Yes
Libgcrypt	Yes	Yes	Yes	Yes	Yes	Yes
Libsodium	No	No	No	No	No	No
Nettle	Yes	Yes	No	No	No	No
OpenSSL	Yes	Yes	Yes	Yes	No	Yes
wolfCrypt	Yes	Yes	Yes	Yes	No	Yes

The cryptographic implementations only with security based hashing algorithms are evaluated in depth in Table 7. Network and communication security may be improved with the use of hash-based methods [32] Figure 3 explain curve.

To ensure that blockchain-based financial and banking solutions work as intended, a comparison of the various implementations' support for SIM cards, HSMs, and smartcards is provided in table 8.

The segments show tabular and graphical representations of the most important factors in the performance of cryptographic methods in Table 9, including the number of rounds, the size of the word, the size of the internal state, the size of the block, and the size of the output in bits. Figure 4 Illustrate this as in the upcoming scenario.

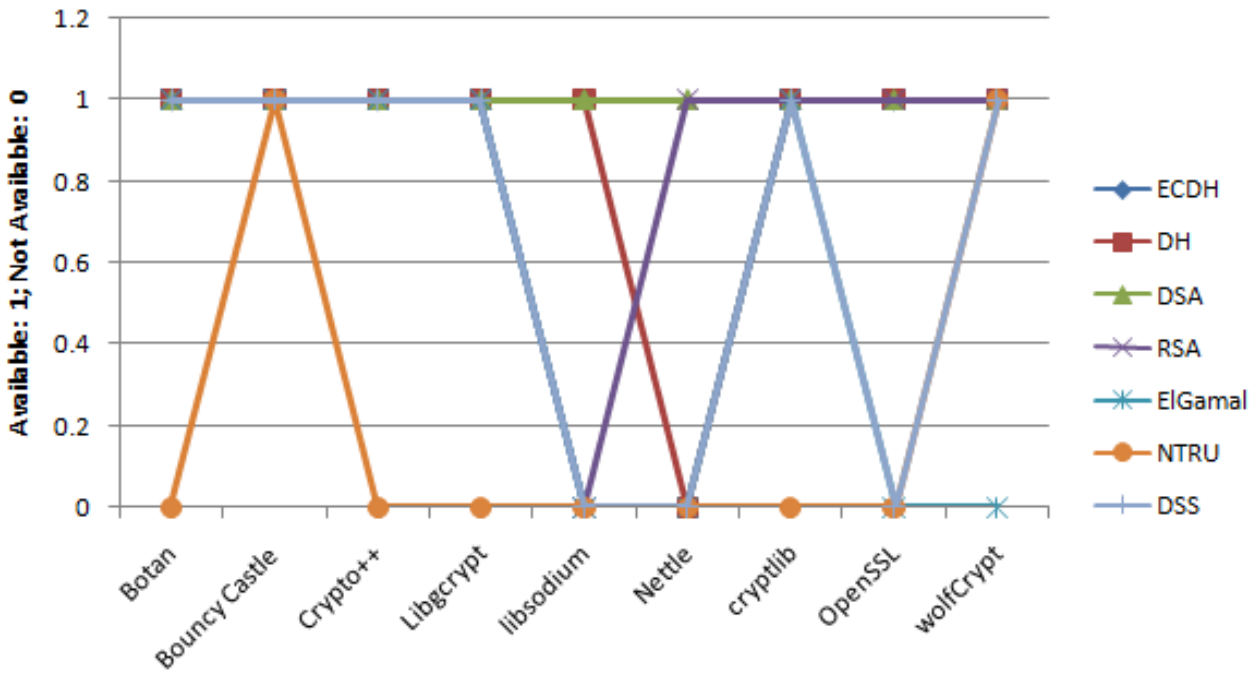

FIGURE 2. Open-Source Cryptography Libraries and Features

Table 8. Implementation details of various Hashing Algorithms

Implementation	MD5	SHA-2	SHA-3	SHA-Y	SHA-Y	RIPEMD-Y6N	Tiger	SHA-Y	Whirlpool	GOST	Stribog	BLAKE2
Botan	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Bouncy Castle	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cryptlib	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
Crypto++	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Libgcrypt	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Libsodium	N	Y	N	N	N	N	N	N	N	N	N	Y
Nettle	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	N
OpenSSL	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
wolfCrypt	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	Y

Table 9. Support for SIM, HSM and Smartcard in the Implementations

Implementation	PKCS #YesYes	PC/SC	CCID
Libsodium	No	No	No
Bouncy Castle	Yes	No	No
Cryptlib	Yes	No	No
wolfCrypt	Yes	No	No
Crypto++	No	No	No
Botan	Yes	No	No
Libgcrypt	Yes	Yes	Yes
OpenSSL	Yes	No	No

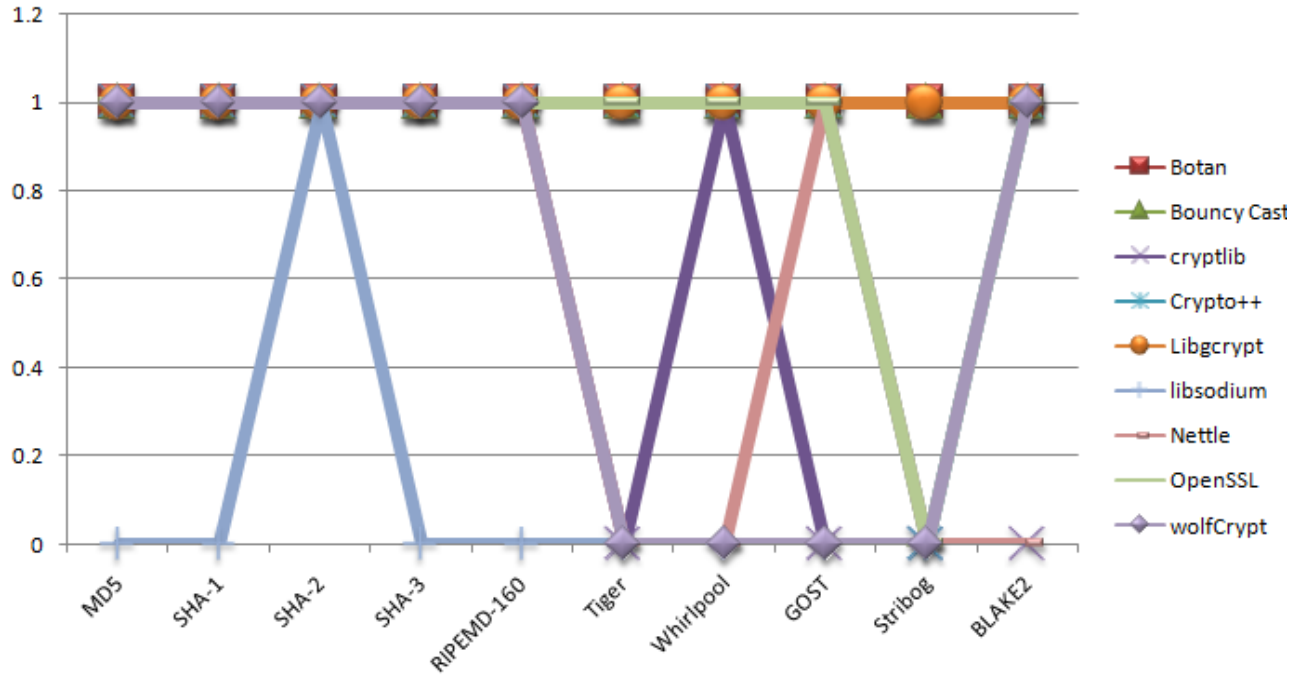

FIGURE 3. Open-Source Cryptography Libraries and Features

Table 10. Evaluation of Cryptography Hash Approaches in Network Environment

Algorithm	Output size (bits)	Word size	Rounds	Internal state size	Block size
HAVAL	128	32	5	256	1024
GOST	256	32	32	256	256
RIPEMD-128/256	128/256	32	64	128/256	512
MD2	128	32	18	384	128
MD5	128	32	64	128	512
PANAMA	256	32	32	8736	256
MD4	128	32	3	128	512
RIPEMD	128	32	48	128	512
RIPEMD-160	160	32	80	160	512
RIPEMD-320	320	32	80	320	512
SHA-0	160	32	80	160	512
SHA-1	160	40	80	160	512
SHA3-224	224	64	24	1600	1152
WHIRLPOOL	512	8	10	512	512
SHA-256	256	56	64	256	512
SHA-3	512	64	24	1600	3200
SHA3-512	512	64	24	1600	576
SHA3-256	256	64	24	1600	1088
SHA3-384	384	64	24	1600	832
Tiger2	128	64	24	192	512
BLAKE2b	512	64	12	1024	512
BLAKE2s	256	32	10	512	256

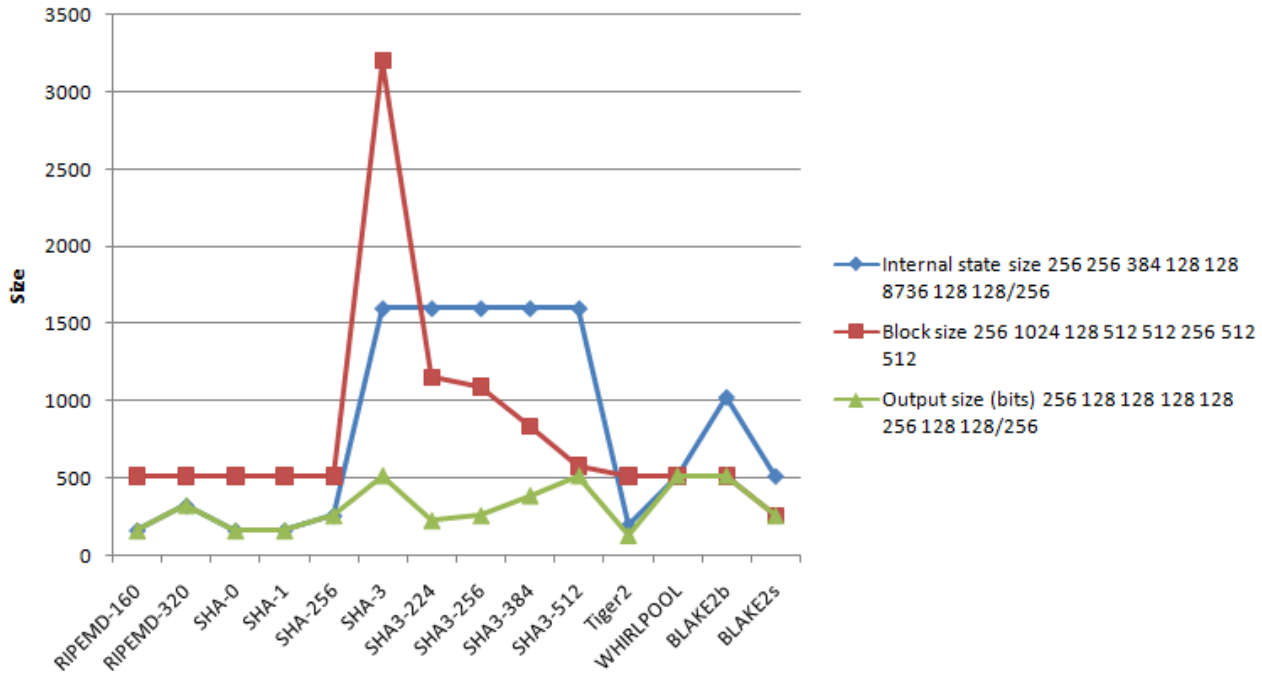

FIGURE 4. Evaluation of Traditional Cryptography Hash Approaches

6. EXTRACTS FROM THE LITERATURE REVIEW

It introduces certificate-less open-key as a solution for securing the IIoT. Rather of revealing the client's typical key, an arbitrary open key is shown in this technique. Compared to Pang's method, the suggested SCF-MCLPEKS strategy is shown to be effective and can be implemented in less time. The researchers of Near Field Communication (NFC) present their methods in this patent [1] [2]. So that a greater degree of security may be attained, the suggested technique makes use of the unique cryptographic key via the NFC and its connection with the EEPROM. [3] This paper introduces Lattice-Based Secure Cryptosystem (LSCSH) for enhanced security applications in densely populated metropolitan settings. In order to improve security, the suggested solution employs a lightweight key exchange system with a multi-layered anchored validation module. With the use of the Access Right Verification Mechanism, the hubs in the communication scenario may be authenticated and given their own unique credentials. In this research, the author proposes a hybrid encryption algorithm, and the analysis shows that it performs well in terms of speed and execution time. To provide both security and faster execution, the suggested model combines the symmetric AES, GCM, and NTRU hilter kilter computations.

In order to improve the safety of the key's communication, the authors of this work provide a lightweight Key foundation plot using an instrument called Identity based accreditation (IBC). The results of the simulation showed that the suggested scheme is secure, adaptable against security attacks, and satisfies the built-in security need for IoT software.

This study proposes a lightweight key assertion standard to facilitate the implementation of more safe and robust security in the vehicle-to-matrix (V2G) system of the Internet of Things. The similarity to the ECC based standard provides support for the suggested paradigm.

In order to safeguard client property values against AA reliant on a 1-out-of-n transparent swap technique, the author of this research presented a CP-ABE plot. Credits The Cipher-usual Text's access configuration has been encrypted using a Bloom Filter for further security. The outcomes proved that the proposed model is more effective and safer than the alternatives. [8] When it comes to security, Datagram Transport Layer Security (DTLS) is where it all begins and ends. In this work presented at the DTLS conference, the authors discuss how to overcome the challenges presented by the key commitment.

This study [9] discusses a variant of RSA called MEMK (Memory productive multi-key). With this paradigm, information may flow in both directions, from the cloud to the Internet of Things and back again. The suggested algorithm combined a non-direct RSA criterion with a Diophantine one. The results of the reenactment showed that MEMK performs better than the control method in terms of encryption and decoding time.

As such, this paper's goal is to manage plot for IoT in the fog and obtain the secure information it requires [10]. It is proposed to do computation using CP-ABE and ABS. When the suggested strategy for client encryption, decoding, and marking is small and essential, it speaks to the plan's appropriateness. The reproducibility findings showed that the suggested approach is safe from the attacks.

The author of this study [11] developed a safe mark based Authenticated key foundation layout to help the Internet of Things (IoT) become more secure and reliable. The suggested plan's security is evaluated with the use of the Burrows AdadiNeedham reasoning, casual security, and casual security confirmation using the widely accepted automated approval of the internet security convention and the NS2 test system.

[12] Given the importance of both assets and execution to an IoT setup, this paper provides recommendations for tradeoffs and enhancements between the two. In addition, a bent Edward bend that is competently endomorphic is used in this study. The usage of endomorphism to hasten the doubling of scalars was also depicted by the author. The 100-piece set provides a range of trade-offs between security and efficiency.

In [13], a lightweight encryption computation called Secure IoT (SIT) was presented by the author. This is a 64-bit number, and it has always needed a 64-bit key in order to complete any given task or decipher any given piece of data. The results of the simulation showed that the suggested scheme provides enough protection after only five rounds of encryption. This study [14] demonstrates a lightweight and safe client validation standard based on the Robin cryptosystem with characteristics of computational asymmetry. Highlights in dynamic security are made easier using the suggested paradigm. The results of the simulation confirmed that the suggested model is practical for progressively adjusting the level of security and productivity that it provides. This research [15] proposes an Elliptic Curve Cryptography (ECC)–based haze registering–based distribute buy in lightweight convention for the Internet of Things infrastructure. ECC reduces computational and capacity overhead by offloading some of the work to remote hubs, which results in shorter key lengths, smaller message sizes, and reduced asset usage. This strategy allows for increased adaptability with less necessities like storing and coordinating. [16] To provide complete safety, this study proposes a method of synchronizing shared keys. When a detecting device in the network acquires a mutual key from a neighboring device, the suggested design synchronizes the shared key without requiring any communication between the devices or the DSM. Comparison to DPBSV and DLSef shows that the proposed strategy is superior. [17] Author suggested an alternative strategy for bolstering heterogeneous WSN's primary assertion and client confirmation. All possible security threats are handled and eliminated by the suggested approach. The findings of the security analysis showed that this model is more secure.

[18] Symmetric Key (S3K) is introduced in this study as a means of protecting information in the Internet of Things (IoT). S3K is a small, lightweight, and practical solution for usage in asset-restricted devices, while also being adaptable to a wide range of other devices.

[19] In this study, we offer a model security architecture with a simple security focus. Addressing the security issue and providing a robust framework are the primary aims of this article. In this study, [20] we present an alternative paradigm for access management in the Internet of Things that makes use of blockchain technology. By using the security and transparency of block chain based encryption like bitcoin, this new framework provides a robust and user-friendly access management tool. This study [21] illustrates the secure system layout with the primary market emphasis on using nearby robotized permitted substances. Our primary goal here is to provide safe system engineering as a foundation for further discussion. The outcome proved that the model's flexibility is superior to that of SSL/TLS. [22] The paradigm of capability-based access control served as the foundation for this study. When applied to an Internet of Things (IoT) situation, this model makes use of IP-based technologies. The balance between safety and speed is improved. [23] An efficient block cypher was the inspiration for the author's CLEFIA proposal. The CLEFIA is a modernized Generalized Feistel network with a hardware implementation and a crypto processor that allows for keys of lengths 128, 192, or 256 bits. [24] To solve this problem, this work proposes a novel hybrid Diffie-Hellman based authentication technique that use both AES and RSA to generate session keys. When compared to current systems, this one reduces communication overhead by 23%.

[25] The author offered a novel strategy for fixing the issue of end-to-end security in the Internet of Things. Cooja simulator is used to simulate the task, and the study discusses the application and security aspects. [26] The method suggested in this research is based on the Lamport one-time pad (OTP) algorithm and the Lightweight identity-based elliptical curve encryption system. The new method uses a one-time password (OTP) and smaller keys to ensure that security is never compromised. [27] In order to address the security concerns inherent in the IoT network, an elliptical curve cryptography technique is developed in this paper. If you need to have private conversations, you can use the ECC optimization that is readily available. This study [28] introduces the benchmarking framework for lightweight block cyphers on a wide variety of embedded platforms. The platform measures the size of the binary code, the amount of RAM, and the footprints.

[33] The primary goal of developing this model architecture was to make the network safer than preexisting ones. Better key management strategies between sensor nodes and a smart gateway were implemented in this suggested concept.

The results showed that there was a 26% decrease in communication overhead. [34] The proposed solution got rid of the security issue by using Elliptic Curve Cryptography's construction and the Hellman key exchange technique. [35] The goal of this article was to offer a data-encryption-based paradigm to simultaneously improve network privacy and decrease encryption time. The primary goal of this research was to design a network protocol with improved safety and privacy. In this work, the author [36] proposes a new architectural approach for implementing an authorization layer for HTTP and CoAP service providers. As a result of its decentralized nature, the suggested method can manage a number of smart objects with a little amount of processing resources. [37] Using public keys, the security presented in this paper protects the Internet of Things. The author begins by outlining the necessary building blocks for private, end-to-end messaging before moving on to explain how public-key cryptography works. Work efficiency is defined as the amount of time spent on computational and communication tasks. [29] In this article, the author unveils the IP-based Internet-of-Thing framework he or she created. As can be seen in the simulation results, this approach significantly decreases the memory overhead by 64%, the computational burden by 97%, and the network transmission by 68%. [30] Lightweight collaborative key exchange strategy for improving Internet of Things network security is presented in this study. The proposed method is superior to the current method since it reduces energy usage by 80%. The author suggested a methodology based on Threshold Cryptography Group Authentication (TCGA) [32]. This model validated the network's available devices to strengthen security and improve reliability. In addition to being a lightweight scheme, this one can also detect and prevent assaults.

[38] In this research, we suggested a method for using CP-ABE on severely underpowered sensor nodes in an Internet of Things setting. This method improves collaboration between the network's sensor nodes. [38] Using the VHDL programming language, the author of this study proposed implementing the Blowfish algorithm on an FPGA. In this research, we investigate the efficacy of the blowfish algorithm and determine the FPGA resource consumption required to run it. The outcomes demonstrated the superior security and faster encryption time of this method. [39] [40]In order to verify the identity of a connected device in a network before granting it access to network resources or a communication channel, this article introduces a lightweight mutual authentication mechanism. To identify and forestall assaults was the primary goal of this study. [41] In this article, we argue for the need of creating a plan for deploying a stripped-down version of the DTLS protocol throughout the Internet of Things. Gaining and enhancing one's own and the network's security was the primary goal of this article.

An Analysis of Prominent Methods Used to Maintain Privacy When Communicating Over the Internet

7. RESULTS, DISCUSSIONS AND ANALYTICS PATTERNS

Using RSA, AES, and MD5 computations with the XOR-based key exchange, a comprehensive evaluation of the various key cryptography methodologies is carried out. Because of the need for a consistent degree of security and trustworthiness across environments and deployment models (Cloud, IoT, Fog, Mist, Edge, and many more), these hybrid approaches have become the norm.

Substantial data should be confused by associated channels, therefore the numbers should not be elaborate. An outsider is required to attest to the general keys' constant quality. In a public key infrastructure, intermediaries may compromise the security of shared information by altering the results of a computation.

Big O can be used to represent the amount of time a computation takes to execute or the amount of storage space it requires (in memory or on a circle), and it always depicts the worst possible outcome. This is evaluated on the more complex Java platform.

Table 11. Parameter Based Evaluation of Algorithms

	XOR	AES	RSA	MD5
Cost Factor (Points)	31	49	87	69
Complexity (Points)	27.74	32.19	71.16	40.17
Execution Time (ms)	0.04	0.05	0.13	0.07
Performance (Points)	93	83	65	71

In order to assess the overall efficacy of the strategies, Table 9 below presents the empirical data gleaned from the evaluations and overall analytics of the outcomes of the implementation.

The assessment's grading criteria are alluded to by the focus. There is no universally accepted measure of uncertainty in the real world. In the course of the Big-O analysis, the computations are evaluated and scored. In order to determine the complex nature of a computation in a simple recipe, huge O documentation allows us to exclude lower-order components and consistent elements. An example of this would be describing the unpredictability of a sorting algorithm as O(n * lg(n)), where n is the total number of items. These are not measured in absolute terms but rather relative ones, such as

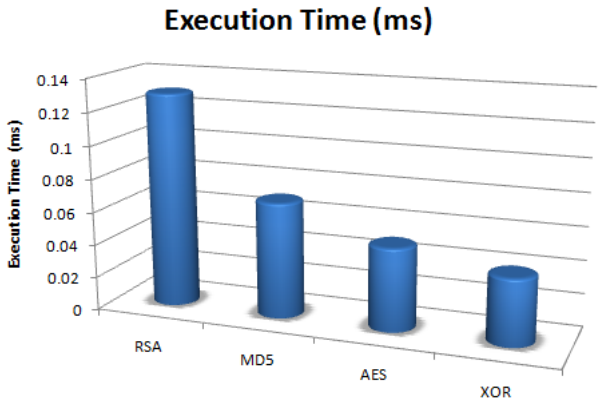

FIGURE 5. Comparative Evaluation of the Approaches

importance or quality. Large-O notation is used to illustrate a calculation's efficiency or unpredictability.

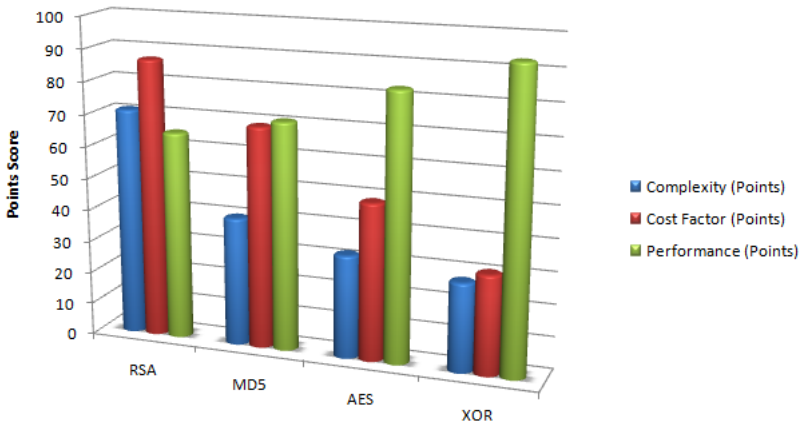

FIGURE 6. Comparative Evaluation of the Approaches

While the alternatives are acceptable, they have higher-level scientific functions and definitions that improve overall security. Using a secret, high-stakes arithmetic method, these computations are shielded from prying eyes. Prime numbers are difficult to factorize, making these computations difficult to solve.

In addition, the general population key is used by various methods to further confuse data, and the key is made publicly available; hence, it is not difficult to disseminate individuals' personal information using the general population key.

8. CONCLUSION

The presented work is having a cavernous analytics on the security mechanisms and associated implementations using dynamic hash based encryption and cryptography algorithms. The work underlines the assorted techniques with the comparative analytics so that the overall performance and effectiveness can be analyzed. In order to provide a thorough comparison of the work done, this manuscript focuses on an empirical analysis of the cryptography techniques utilized in the advanced wireless scenarios of the Internet of Things (IoT), where different approaches are evaluated against one another. Several methods and techniques for achieving a greater level of accuracy and cumulative performance metrics in encrypted communication are discussed in this manuscript.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] M. Ma, D. He, N. Kumar, K. K. Choo, and J. Chen, "Certificate-less searchable public key encryption scheme for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 759–67, 2018.
[2] P. H. Minatel, S. H. Lee, and B. S. Pinto, "Boeira FC, inventors; Samsung Electronica da Amazonia Ltda, assignee. Method for Verifying Authenticity, Configuring Network Credentials and Cryptographic Keys for Internet Of Things (IoT) Devices Using Near Field Communication (NFC)," 2018.
[3] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena *LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. IEEE Communications Magazine*, vol. 56, pp. 24–32, 2018.
[4] D. M. Trivedi and T. J. Raval, "Proposed Cryptographic Approach for Securing IOT Device," 2018.
[5] A. S. Sani, D. Yuan, P. L. Yeoh, W. Bao, S. Chen, and B. Vucetic, "A Lightweight Security and Privacy-Enhancing Key Establishment for Internet of Things Applications," *In2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2018.
[6] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2526–2562, 2018.
[7] Q. Han, Y. Zhang, and H. Li *Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. Future Generation Computer Systems*, vol. 83, pp. 269–77, 2018.
[8] U. Banerjee, C. Juvekar, A. Wright, and A. P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in iot applications," *InSolid-State Circuits Conference-(ISSCC)*, pp. 42–44, 2018. IEEE.
[9] C. Thirumalai and H. Kar *Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices. InPower and Advanced Computing Technologies (i-PACT*, pp. 1–6, 2017. IEEE.
[10] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with Cipher-Text update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941–50, 2017.
[11] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3071, 2017.
[12] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, and I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things," *IEEE Transactions on Computers*, vol. 66, no. 5, pp. 773–85, 2017.
[13] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "Sit: A lightweight encryption algorithm for secure internet of things," 2017.
[14] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–92, 2017.
[15] A. A. Diro, N. Chilamkurti, and N. Kumar *Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing. Mobile Networks and Applications*, vol. 22, pp. 848–58, 2017.
[16] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A synchronized shared key generation method for maintaining end-to-end security of big data streams."
[17] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl *An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks*, vol. 36, pp. 152–76, 2016.
[18] S. Raza, L. Seitz, D. Sitenkov, and G. Selander, "S3K: scalable security with symmetric keys-DTLS key establishment for the Internet of things," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1270–80, 2016.
[19] X. Huang, P. Craig, H. Lin, and Z. Yan *SecIoT: a security framework for the Internet of Things. Security and communication networks*, vol. 9, pp. 3083–94, 2016.
[20] A. Ouaddah, A. A. Elkalam, A. Ouahman, and A *FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks*, vol. 9, pp. 5943–64, 2016.
[21] H. Kim, A. Wasicek, B. Mehne, and E. A. Lee, "A secure network architecture for the internet of Things based on local authorization entities. InFuture Internet of Things and Cloud (FiCloud)," *IEEE 4th International Conference on*, pp. 114–122, 2016.
[22] J. L. Hernández-Ramos, A. J. Jara, L. Marín, S. Gómez, and A. F, "DCapBAC: embedding authorization logic into smart things through ECC optimizations," *International Journal of Computer Mathematics*, vol. 93, no. 2, pp. 345–66, 2016.
[23] G. C. Bae and K. W. Shin, "An efficient hardware implementation of lightweight block cipher algorithm CLEFIA for IoT security applications," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 2, pp. 351–359, 2016.
[24] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," *Computers & Electrical Engineering*, vol. 52, pp. 114–138, 2016.
[25] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and G. R. Oscar *Object security architecture for the Internet of Things. Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.
[26] V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)," *InInformation Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on*, pp. 1–6, 2015.
[27] L. Marin, M. P. Pawlowski, and A. Jara *Optimized ECC implementation for secure communication between heterogeneous IoT devices. Sensors*, vol. 15, pp. 21478–99, 2015.
[28] D. Dinu, L. Corre, Y. Khovratovich, D. Perrin, L. Großschädl, J. Biryukov, and A, "Triathlon of lightweight block ciphers for the internet of things," *Journal of Cryptographic Engineering*, 1920.
[29] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based Authentication and Authorization for the IP-based Internet of Things. InSensing, Communication, and Networking (SECON)," *Eleventh Annual IEEE International Conference on*, pp. 284–292, 2014.
[30] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent *Lightweight collaborative key establishment scheme for the Internet of Things. Computer Networks*, vol. 64, pp. 273–95, 2014.

[31] O. A. Hassen and H. Ibrahim, "Preventive Approach against HULK Attacks in Network Environment," *International Journal of Computing and Business Research*, vol. 7, 2017.
[32] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)."
[33] S. R. Moosavi, T. N. Gia, A. M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Computer Science*, vol. 52, pp. 452–461, 2015.
[34] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," *InProceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, pp. 37–42, 2015.
[35] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, W. Hu, and Talos, "Encrypted query processing for the internet of things," *InProceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, pp. 197–210, 2015.
[36] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari *Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. IEEE sensors journal*, vol. 15, pp. 1224–1258, 2015.
[37] H. Shafagh and A. Hithnawi, "Security comes first, a public-key cryptography framework for the internet of things," *2014 IEEE International Conference on*, pp. 135–136, 2014.
[38] L. Touati, Y. Challal, A. Bouabdallah, and C-Cp-Abe *Cooperative Cipher-Text policy attribute-based encryption for the internet of things. InAdvanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on*, pp. 64–69, 2014. IEEE.
[39] K. N. Prasetyo, Y. Purwanto, and D. Darlis *An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA. InInformation and Communication Technology (ICoICT)*, pp. 75–79, 2014. IEEE.
[40] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment. InTrust, Security and Privacy in Computing and Communications (TrustCom)," *IEEE 13th International Conference on*, pp. 205–211, 2014.
[41] V. Lakkundi and K. Singh, "Lightweight DTLS implementation in CoAP-based Internet of Things," *InAdvanced Computing and Communications (ADCOM)*, pp. 7–11, 2014.
[42] M. Neamah, "Fuzzy logic integrated security aware algorithm for vulnerability avoidance in network environment," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, pp. 785–794, 2018.