JOURNAL PUNJAB ACADEMY OF SCIENCES (Peer Reviewed Open Access Journal)
JPAS, 23: 16-32 (January-December, 2023)
Available online at www.jpas.in
ISSN 2229-7014 (P)

INTEGRATED ENCRYPTION SCHEME IN FOG COMPUTING FOR E-HEALTHCARE APPLICATION

Priyanka Rajan Kumar[1] and Sonia Goel[2]

[1]Research Scholar, Department of Computer Science
Punjabi University, Patiala,(147001) Punjab, India.
E-mail: srpriyankass@gmail.com

[2]Department of Electronics and Communication Engineering,
Punjabi University, Patiala (147001) Punjab, India.

ABSTRACT

E-Health is a system of providing health services by making use of electronic technologies. They provide improved, flexible, and affordable health services to a large population, especially in situations like a pandemic. The IoT is helping them to connect, generate and share a huge amount of data. This system of online sharing of health records and advice is generating data at rapid growth. This large data is to be managed in terms of storage, processing, transmission, privacy, and security. The cloud came up as a source of big data management but when it came to latency and bandwidth consumption, a system of processing near the edge came as a Fog Computing with distributed processing, reduced delay, and less bandwidth. The Fog is near the generation of data that provides benefits like location awareness, heterogeneity, real-time access, wireless access, and scalability. Here the security of sensitive data is a prime factor. Security can be achieved with cryptography. The paper implemented RSA, BLOWFISH, AES, and Integrated Encryption Scheme of (RSA+BLOWFISH) and (RSA+AES) combination security algorithms in the Fog-enabled E-Healthcare system. The comparison of performance is done on the basis of key size, encryption-decryption time, and throughput. It is found that BLOWFISH has the least encryption-decryption time and more throughput in a single encryption scheme. In the Integrated Encryption Scheme, the (RSA+AES) combination has improved performance among the two combinations. So, to achieve the security of the E-Health system in the Fog computing environment it is more efficient to use Integrated Encryption Scheme.

Keywords: Fog Computing, Internet of Things (IoT), Rivest, Adi Shamir, and Leonard Adleman (RSA), Advanced Encryption Standard (AES) Transport Layer Security (TLS), BLOWFISH.

INTRODUCTION

E-Health is a system of using the Internet and its technologies to enhance the health support system. The internet is the ground for the working the of E-Health system. Its development has led to the development of new ways of providing healthcare as well as successive scopes in healthcare (Robert 2017). People around the globe have faced many difficulties regarding healthcare during the pandemic period. The people were to stay at home for the safety of their health. Everyone was told to stay safe at home. But the people who required health support, need to reach the health service providers. The people were to take health advice from the experts but they were not allowed to go out. During the pandemic period, there were patients who needed continuous monitoring and chronic patients who require immediate advice. The healthcare professionals were advising the people who are in better health conditions to stay safe at home and were giving automated advice to them through web technologies. They were trying to filter out the people coming to the hospitals so as to avoid the spreading of the pandemic. The highly automated infrastructure made use of AI and cloud computing paradigm. The advanced healthcare system made use of portals, and application software to provide health advice to the concerned patients. The E-Health system has IoT as the backbone. The Internet of Things has made it feasible to design such every time everywhere connectivity feasible. Our E-Health services are also working on the basic architecture of the IoT paradigm. The IoT is an innovative communication infrastructure that has the potential of providing limitless benefits to our society (Robert 2017). The IoT is intended to reduce data entry tasks and make use of sensors for the collection of data from the environment and allows storage and processing of the data (Giang 2014, Hany 2018). The IoT has limited computation power in terms of processing and storage, it faces many problems such as performance, security, privacy, and reliability (Hany 2017, Peng 2018). The IoT brings many applications that provide advantages to society as a whole. These IoT devices have heterogeneous nature and generate a huge amount of data. This big data is required to be analyzed for decision-making. Therefore, the IoT needs a platform for the processing and storage of data. The huge amount of data generated by connected individuals and organizations needs storage and processing capabilities. The cloud provides a processing platform for data. This has led to the use of cloud computing platform that offers data storage and computing facility. But there are certain constraints such as latency, network bandwidth, and centralized control that aroused a need for an environment for processing and storage that reduces delay as well as network bandwidth. This can be achieved by a paradigm of computing known as Fog Computing. Fog Computing is a term coined by CISCO (Bonomi 2012). Fog provides advantages to many different fields. The IoT is one of them where Fog provides services of processing and storage of real-time data near the generation of data. The fog due to lesser distance and distributed computing infrastructure provides improved performance in terms of reduced latency, and lesser network bandwidth consumption (Peter 2015). The data collected from sensors is sent to edge devices for processing and storage instead of sending them to the cloud (Rovatsos 2017). Fog computing with IoT is creating a service called as Fog as a Service (FaaS) (Yang 2017). Fog computing is a communication infrastructure that provides benefits of location awareness, heterogeneity, real-time access, wireless access, and scalability. Fog provides aggregation, data filtering, and analysis at the edge of the network which results in improved quality of service. The fog acts as a middle layer in the three-tier architecture of the Internet of Things. Its security plays an important role in the security of the communication architecture (Miao 2018). Fog computing can scale down the response time of the user by 20%, and traffic load on the network by 90%. Fog can even reduce the latency of real-time applications by 50% (Zhang 2017). Fog Computing is a promising solution for expertly serving IOT applications and their data security is a prerequisite challenge (Sookhak 2018). The threat to data becomes more critical when resource-constrained devices transfer sensitive data as these devices are connected through the internet (Mohd 2018).

Fog Computing vs. Cloud Computing

Cloud computing provides on-demand services. It provides processing and storage services for big data. It provides a centralized processing infrastructure. The Fog came up as distributed computing architecture. Table 1 shows the main difference between Fog computing and Cloud computing.

Table 1. Difference between Fog computing and Cloud computing

Features	Cloud computing	Fog computing
Latency (Robert 2017)	High	Low
Security (Giang 2014)	Less security than fog computing	High security
Speed (Hany 2018)	Depends on VM connectivity	Higher speed
Mobility	Limited	Higher Mobility

Geographical distribution (Yang 2017)	Centralized	Decentralized and distributed
Communication mode	IP network	Wireless Communication
Responsiveness	low	high

Fog has lesser latency, more security, high security, higher mobility, and distributed geographical distribution as compared to the cloud. So, Fog computing provides more efficient E-health services. The data is huge and heterogeneous in nature. The data is available online and it is vulnerable to attacks (Mohammed 2018) . These network security threats can affect the sensitive medical data being shared through E-health services. The E-health system needs to be safe to share sensitive data. Medical records such as essential healthcare records of patients, expert advice from healthcare experts, and their medical prescriptions should be secure enough. Trust maintenance is mandatory so that regular legitimate as well as authenticate relationships with the patients can be made. So, the security of the data is very much essential. Security can be achieved by cryptography (Strauss 1998). Data encryption is very much important for ensuring the privacy of the sensitive data stored on Fog nodes in the entrusted online environment. For the institutional as well as patient personal health data details efficient security algorithm is required. In this respect, three algorithms RSA, BLOWFISH, and AES are compared. Furthermore, an integrated encryption scheme (RSA+BLOWFISH) and (RSA+AES) combinations are also applied in the same Fog Computing environment to achieve the security of the sensitive data.

RELATED WORK

An Attribute Based Encryption (ABE) scheme is proposed (Alrawais 2017) to secure fog communication where an efficient key exchange protocols based on cipher text policy attribute-based encryption (CP-ABE) to establish secure communication among participants is used. In this the digital signature and CP-ABE methods are used to achieve the primary security goals of confidentiality, authentication, verifiability and access control. A further comparison is made with the certificate-based scheme to illustrate its efficiency. The proposed scheme does not involve the transmission cost because it does not require to exchange certificates or any identity information as attributes are linked with the private key. The scheme is more efficient and secure than the certificate-based scheme.

The security in Fog Computing is achieved by Advanced Encryption Standard (AES) (Akhilesh 2016). The performance of the encryption is evaluated for accuracy with time, user load, response time, memory utilization. The objective of the study is to apply AES encryption to render security at the Fog layer of the Cloud-IoT system. Performance is evaluated for different data sizes on Fog device. The data is categorized as small data (Data set-I 500KB), large data (Data set-II 5MB) and bigger data (Data set-III 10MB). The CPU utilization is same for small data set. The CPU utilization varies for large and bigger data set. A further comparison is made by using mobile and laptop for calculating the processing time. It is also concluded that memory utilization is same for every device having same RAM.

To secure the data between the user device and Fog network a privacy preservation procedure is proposed (Kulkarni 2014). Security of the data in transmission is of concern in Fog computing. A modified ElGamal algorithm is applied for key generation. The data is encrypted before sending it to the cloud along with the encrypted key generated with modified ElGamel algorithm. This provides better security than the existing security solutions due to the cipher key along with encrypted data. The method also increases the execution speed that leads fast authorized access to the data (Sowjanya (2017).

A study on securing IoT-Fog computing gateway communication was done. In this work a comparison on the performance of RSA and ECC is done. The study provides three contributions for the security of resource constrained environment. First, it provides the basics of security performance and capabilities of Internet of Things (IoT) gateway. Second, hardware testbeds were created for implementations of RSA and ECC to measure power consumption and throughput of system. Third, the impact of transport layer security (TLS) in IoT communication was evaluated to measure the difference between RSA and ECC in terms of security, scalability, power consumption and throughput. It is found that ECC has 50% reduction in power consumption and double throughput than RSA (Suárez 2017).

The security of Fog Computing with the IOT environment has been discussed (Alrawais 2017). A procedure to enhance the security and privacy among IoT devices for distributed services has been employed with the help of Fog. A case study in IoT environment has solved security and privacy concerns with Fog Computing. A review of Fog Computing applications has been done to identify the security and privacy concerns. It has been discussed that Fog applications emphasize functionality rather than security and privacy concerns that make them vulnerable to attacks. The study also focused on the impact of security and privacy breaches and possible solutions for providing privacy of the data have been proposed (Saad 2017).

A ciphertext-policy attribute-based encryption (CP-ABE) to the data on Fog Computing has been established. It secures the data based on the attributes. These attributes are required to encrypt and decrypt data (Alrawais 2017, Huang 2017 and Zhang 2017). A study (Nishat 2020) uses identity-based cryptography for securing the data on Fog Computing. These ID-based cryptographic operations are having higher computational cost as decryption phase requires more complex operations. These ABE, CP-ABE and ID-based cryptography techniques makes the processing cost higher that is resource intensive. These techniques are not very much suitable for Fog nodes.

A study has proposed ECC based proxy re-encryption for Fog to things communication. The analysis on the encryption decryption time, throughput and efficiency has also been done. ECC is found to be more secure and lightweight due to smaller key size and performance. It has also been proved that Fog Computing require lightweight cryptography technique due to its resource constrained environment (Diro 2018).

The Fog Computing data security in the data transmission is achieved through blockchain. The Fog node clusters are maintained and the access policy is according to block chain-based Fog node clusters (Ansari 2020). A security framework for Fog computing to enhance the IoT security has been developed. A single point of aggregation and lattice cryptography is used for security on Fog. Two levels of cache are implemented for improving efficiency. This model still needs memory management and resource optimization for enhancing the performance of system (Kumar 2020).

An anonymous attribute-based broadcast encryption has been proposed (Zhang 2020). The system has a property of secret access of data to several participants that follow the access policy. This sharing of the data is reliable as it monitors the vulnerabilities as well as the performance of the system. A low-power AES encryption architecture has been proposed. It has reduced power consumption because it uses a lower power S Box. The system has increased security with the help of key management that will also handle eavesdroppers and replay attacks (Tsai 2019). A password-based encryption (PBE) scheme is used to protect sensitive data. The system also presented performance metrics and experimental results are also provided (Mustacoglu 2020).

Table 2 provides the analysis of encryption techniques used in Fog Computing. The analysis gives a view of the various methods being employed in the Fog Computing environment to achieve real-time processing of sensitive data as well as security and privacy of data. In the table, various encryption techniques being applied in the Fog environment and their results are also discussed.

Table 2. Analysis of Encryption Techniques used in Fog Computing

Sr No.	References	Propounded System	Encryption Technique	Results
1.	Alrawais	An Attribute-Based	Digital	The primary security

	(2017)	Encryption Scheme to Secure Fog Communications	Signature CP-ABE	goals: confidentiality, authentication, verifiability and access control are achieved and a comparison is made with the certificate-based scheme to illustrate its efficiency.
2.	Akhilesh (2016)	Security in Fog Computing through Encryption	AES	Performance of the system is evaluated at different data sizes.
3.	Kulkarni (2014)	Preserving privacy in sensor-fog networks.	Feature Reduction Techniques	The research has an importance in terms of safeguarding personal and sensitive data in transit. The suggested method can be improved by opting an encryption and key management algorithm to maintain privacy.
4.	Sowjanya (2017)	Security Framework for sharing data in Fog Computing.	Modified ElGamal	Increases the execution speed that leads fast authorized access to the data.
5.	Suarez (2017)	A practical evaluation of a High Security Energy efficient gateway for IOT – Fog Computing Applications	Performance evaluation of ECC and RSA	ECC is suitable for resource constrained environment where energy efficiency and throughput are essential The power consumption in ECC is 50% than RSA and throughput almost doubles.
6.	Alrawais, (2017)	Fog computing for the internet of	Security and privacy on	Procedure to enhance the security and privacy

		things: Security and privacy issues.	Fog	among IOT devices for distributed services has been employed
7.	Saad (2017)	Fog computing security: a review of current applications and security solutions.	Security and Privacy	Impact of security and privacy breaches and possible solutions for providing privacy of the data has been proposed
8.	(Alrawais 2017, Huang 2017 and Zhang 2017)	An attribute-based encryption scheme to secure fog communications.	CP-ABE	It secures the data based on the attributes
9.	Diro (2018)	Analysis of lightweight encryption scheme for fog-to-things communication.	ECC, RSA	ECC is found to be more secure and lightweight due to smaller key size and performance.
10.	Nishat (2020)	An identity-based encryption scheme for data security in fog computing.	ABE, CP-ABE and ID-based cryptography	The processing cost higher that is resource intensive. These techniques are not very much suitable for Fog nodes.
11.	Ansari (2020)	A cooperative computing strategy for blockchain-secured fog computing.	Block chain	Fog node clusters are maintained and the access policy is according to block chain-based Fog node clusters
12.	Kumar (2020)	A novel framework for fog computing: Lattice-based secured framework for cloud interface.	Lattice based	Single point of aggregation and lattice cryptography is used for security. Model still needs memory management and

				resource optimization
13.	Zhang (2020)	An efficient and secure data transmission mechanism for Internet of vehicles considering privacy protection in fog computing environment.	Attribute - based broadcast encryption	Sharing of the data is reliable
14.	Tsai (2019)	Low-power AES data encryption architecture for a LoRaWAN.	AES	Improved efficiency
15.	Mustacoglu (2020)	Password-based encryption approach for securing sensitive data.	PBE	Good to protect sensitive data

IMPLEMENTATION

The Fog nodes are used for outsourcing sensitive data, this decreases the control of the data by the user, and hence the data becomes vulnerable to security and privacy threats [16]. To solve the security and privacy risk to the data, many complex and resource-consuming security techniques are applied to the IoT-Fog network. But these lead to high computational costs, affect the lifetime of devices as well as increase latency. This can be handled by applying lightweight encryption techniques on resource-constrained Fog nodes for resource optimization along with the security and privacy of data.[17] The fog nodes are resource-constrained devices which is why the security techniques used should be such as they are lightweight and provide resource optimization along with the privacy of data. Information security has held confidentiality, integrity, and availability known as CIA triad to be core principles for the last twenty years [28]. Information security is achieved by cryptographic techniques. They are broadly classified into three types: Symmetric, Asymmetric, and hash functions. Cryptography provides the security services needed for achieving safe and protected information system. The conventional cryptographic system was good to achieve security on general purpose computers. These systems produced reduced performance and has given lower efficiency when implemented on resource constrained environment. This has aroused a need of new techniques of cryptography denoted as lightweight cryptography. These techniques provide integrity, privacy and trust along with other services by using public and private cryptographic methods. The lightweight cryptography is a technique to provide security in a constrained environment [28]. It provides security services with low-cost encryption algorithms. These algorithms give balance between performance, security and size of implementation.

The Fog environment has been created for the implementation of security algorithms. The sensor senses the data, the data is encrypted at the sensor only to keep the confidentiality and integrity of the data. The encrypted data is sent through the fog device and gateway to the actuator for taking the action as per the processed data.

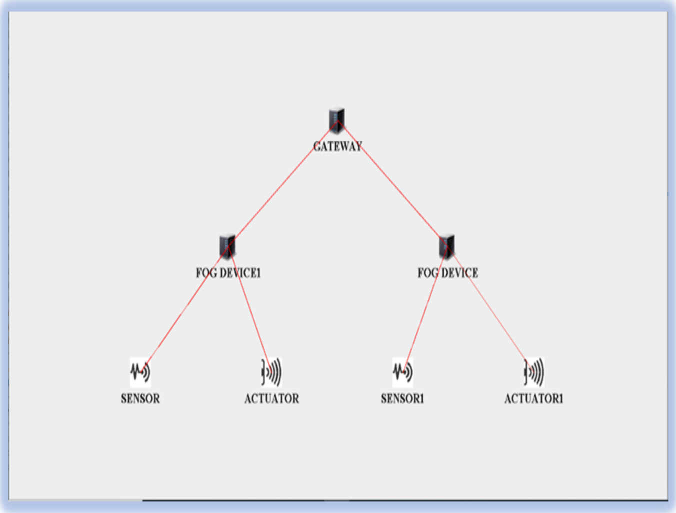

Figure 1: Topology for Fog Environment

Figure 1. depict the topology created for the Fog communication environment. The algorithms are applied on the data in this environment and various parameters are measured to study the performance of the security algorithms interms of processing time and cost.

This paper aims to compare the encryption algorithms that are used for the security of Fog computing and E-healthcare system. The algorithms that are compared are RSA, BLOWFISH and AES, the basis is key size, processing time and throughput. The research has three stages:

Stage 1: This stage will apply security algorithm in Fog environment to measure the parameter values for performance comparison among RSA, BLOWFISH, AES algorithms.

Stage 2: This stage will combine symmetric and asymmetric algorithms to form Integrated Encryption Scheme and measure parameter values among the hybrid combination algorithms.

Stage 3: This stage will compare the performance parameters of single algorithms and Integrated encryption scheme. This stage compares them to conclude that Integrated Encryption Scheme provides more security with improved performance parameters.

RSA (Rivest, Adi Shamir, and Leonard Adleman) Algorithm: It is an asymmetric cryptography algorithm, it uses a *public* key and a *private* key (two different, mathematically linked keys). The names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

Algorithm 1: Structure of RSA algorithm

1. **Select P, Q** where P and Q are prime numbers, P! = Q.
2. **Calculate n**, where n = P *Q.
3. Calculate $\Phi(n)$, where $\boldsymbol{\Phi(n) = (P-1) * (Q-1)}$.
4. Select random E such that gcd($\Phi(n), E$) = 1 and 1<E< $\Phi(n)$.
5. Calculate D such that **d.e ≡ 1 (mod $\boldsymbol{\Phi(n)}$).**
6. Public key = {E, n}
7. Private key = {D, n}
8. Let m be a Plaintext message then cipher text C is $\mathbf{C = m^e \bmod n}$
9. Plaintext message m is $\mathbf{m = c^d \bmod n}$

RSA algorithm is applied in the Fog computing environment. The data of different sizes have been used for encryption and decryption to see the processing time. Figure 2 shows the graph of the encryption decryption time of RSA in the Fog computing environment. The data size of 1 KB,100KB, and 1000KB are taken to see the performance of the system.

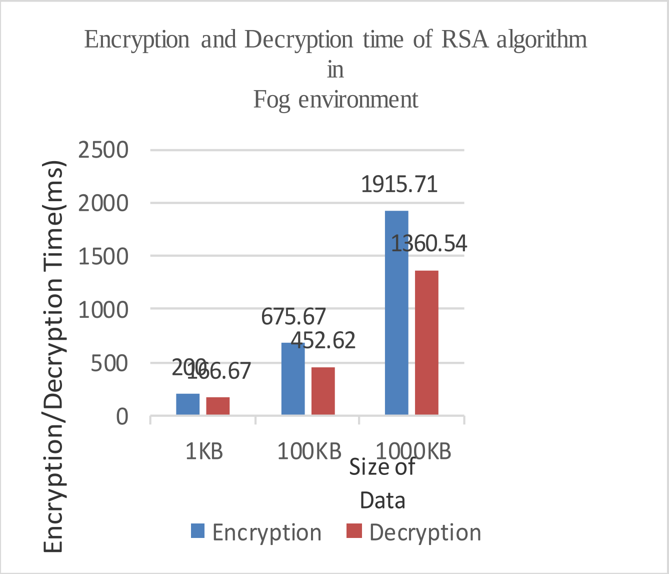

Figure 2: Encryption and Decryption Time of RSA algorithm in Fog environment

The throughput of encryption decryption is also calculated for the RSA algorithm in a fog environment. Figure 3 shows the graph of encryption decryption throughput of the RSA algorithm.

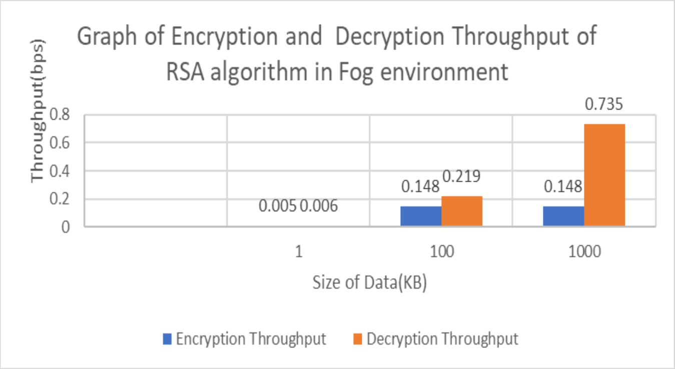

Figure 3: Throughput for RSA algorithm in Fog environment

BLOWFISH Algorithm:

Blowfish is the symmetric encryption algorithm created by Bruce Schneier in 1993. Symmetric encryption uses a single encryption key to both encrypt and decrypt data. The sensitive data and the symmetric encryption key are utilized within the encryption algorithm to turn the sensitive data into ciphertext. Blowfish, along with its successor Twofish, was in the running to replace the Data Encryption Standard (DES) but were not able due to the small size of its block. Blowfish uses a block size of 64, which is considered wholly insecure. Twofish fixed this issue, by implementing a block with a size of 128. Blowfish is much faster than DES, but it trades in its speed for security.

Figure 4 shows the Fiestal structure of the BLOWFISH cipher. BLOWFISH is significantly faster than DES and IDEA and is unpatented and available free for all uses. However, it couldn't completely replace DES due to its small block size, which is considered insecure. Twofish, its successor, addressed the security problem with a larger block size of 128 bits. Nonetheless, full Blowfish encryption has never been broken, and the algorithm is included in many cipher suites and encryption products available today. The BLOWFISH algorithm has been implemented in the Fog environment to see the performance of parameters. Encryption/ Decryption time is calculated for various sizes of data. The graph of the encryption-decryption time is shown in Figure 5.

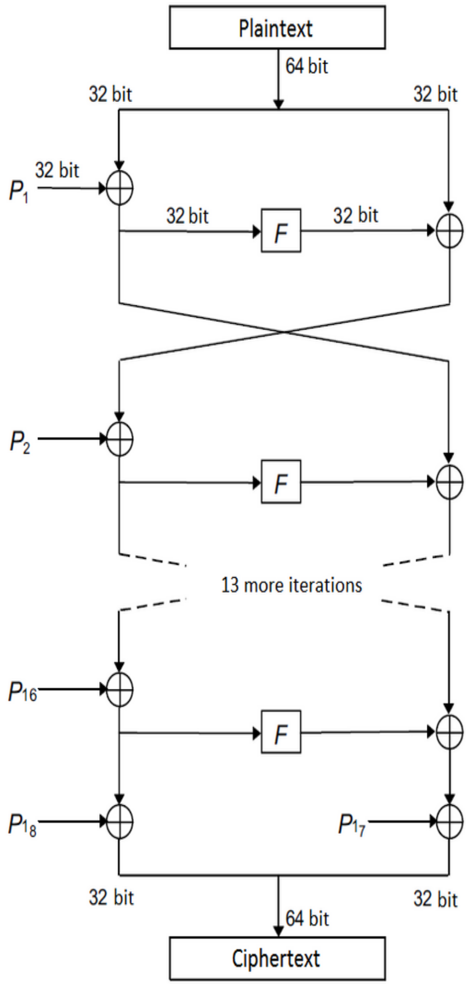

FIGURE 4. FIESTAL STRUCTURE OF BLOWFISH CIPHER

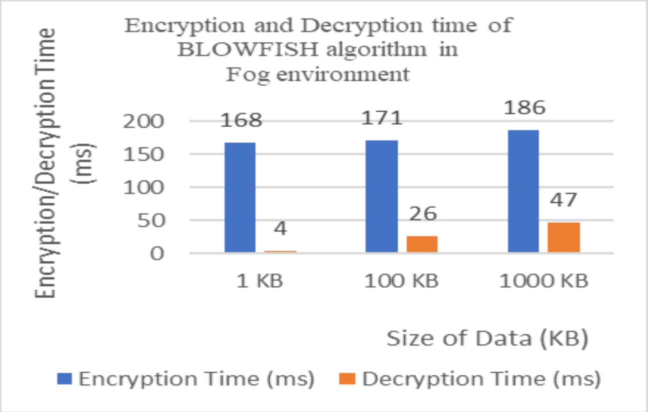

Figure 5: Encryption and Decryption Time of BLOWFISH algorithm in Fog environment

The Encryption decryption throughput is calculated for the BLOWFISH algorithm in the Fog environment. Figure 6 shows the graph of the encryption-decryption throughput of the BLOWFISH algorithm.

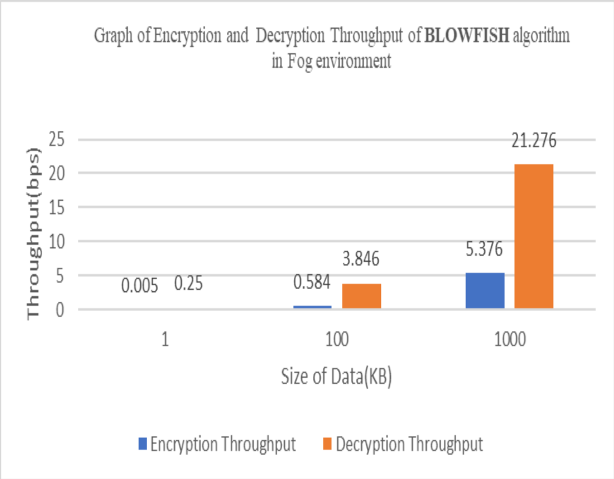

Figure 6: Encryption and Decryption Throughput of BLOWFISH algorithm in Fog environment

Advanced Encryption Standard (AES) Algorithm:

It is a type of symmetric, block cipher encryption and decryption algorithm. It works with key size 128, 192, and 256 bits. It uses a valid and similar secret key for both encryption and decryption. In AES, the block cipher is used. It means that the data to be encrypted is converted into blocks for encryption. The original data value is encrypted using different bits of padding such as 128, 192, or 256 bits. While decrypting a message, the reverse process of encryption is followed. It requires the value of the secret key in order to acquire the original message.

Operation of AES: AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key.

Algorithm 2: Structure of AES algorithm

```
Function AES (byte in [16]),
    key_arrayround_array([Nr+1])
byte state[16]
state=in
AddRoundKey(state,round_key[0])
For i=1 to Nr-1 do
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, round_key[i])
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, roundKey[Nr])
out=state
return out
```

AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The AES algorithm is implemented to see the performance of the algorithm with varying data sizes. The graph is also drawn for the encryption-decryption time of the AES algorithm and is represented in Figure 7.

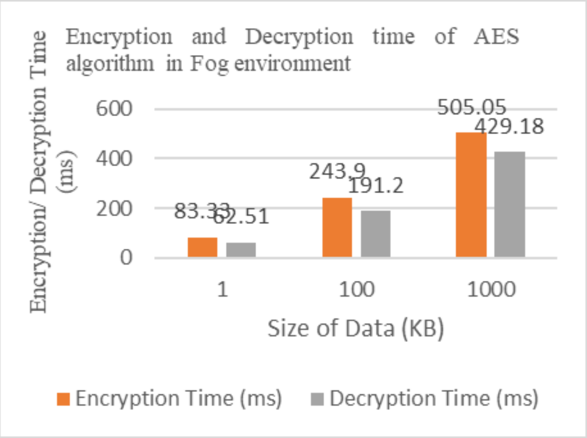

Figure 7: Encryption and Decryption Time of AES algorithm in Fog environment

The throughput is also calculated for the AES algorithm. The graph of the throughput of the AES algorithm is shown in Figure 8.

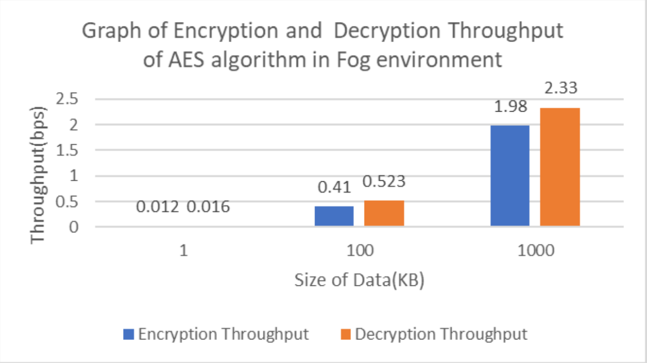

Figure 8: Encryption and Decryption Throughput of AES algorithm in Fog environment

The RSA, BLOWFISH, and AES algorithms are applied in the Fog environment to see their performance for the security of E-healthcare data. The aim here is to measure the encryption-decryption time, throughput, and key sizes to draw a comparison between them to find which is the more secure and faster algorithm.

Comparison between RSA, BLOWFISH, and AES Algorithms: A comparison of RSA, BLOWFISH and AES is shown in Table 3. The comparison is drawn on the basis of cipher type, key size, rounds, block size, level of security, and encryption speed. It is clear that the key size of RSA depends on the number of bits on a module with only one round and BLOWFISH has a variable key size of 32-448 bits with 16 rounds, whereas AES can have 128,192,256 bits of the key size with 10,12,14 rounds respectively. The level of security is good in RSA whereas it is excellent in case of BLOWFISH and AES.

Table 3. Comparison of RSA, BLOWFISH, AES algorithms

Parameters	**RSA**	**BLOWFISH**	**AES**
Cipher Type	Asymmetric	Symmetric	Symmetric
Development	1978	1993	2001
Key Size	The key size depends on the number of bits on a module	32-448 bits	128,192,256
Rounds	1	16	10,12,14
Block Size(bits)	Variable block size	4 bits	128 bits
Level of Security	Good level of Security	Excellent Security	Excellent Security
Encryption Speed	Average	Faster	Faster

3. **Integrated Encryption Scheme (IES):** The E-Healthcare system is a system of providing automatized health services with greater expertise, low latency, and larger geographical coverage. The cloud due to centralized processing infrastructure needs a platform of distributed processing. This is provided by Fog computing. The fog nodes that have distributed workloads can handle larger processing tasks with more mobility. This near-the-edge computing system provides quick health services to users. The confidential information can be transferred through Fog nodes. To secure the private information stored on mobile Fog nodes, an integrated security system has been developed that combines the features of symmetric and asymmetric encryption techniques to provide an efficient encryption scheme. The combination of the algorithm provides less processing time and better response. The Integrated Encryption scheme uses two combinations.

(I) First combination (RSA + BLOWFISH) Algorithm

(II) Second combination (RSA + AES) Algorithm

(I) First combination (RSA + BLOWFISH) Algorithm: An integrated security scheme using (RSA+BLOWFISH) algorithm is implemented in the Fog environment to analyse the performance of the algorithm. This is a combination of asymmetric and symmetric algorithms. The integrated encryption scheme has been applied to primarily compare the performance of the combination algorithm with the single algorithm to attain greater security with improved performance. Encryption decryption time is calculated along the throughput and it is found that the integrated encryption scheme shows improved performance and is more efficient. The encryption and decryption time of the integrated encryption scheme is calculated on the data sizes of 1KB, 100KB, and 1000KB respectively. The encryption-decryption time of the integrated encryption scheme is found to be less than the single encryption scheme. The graph of encryption decryption time is shown in Figure 9.

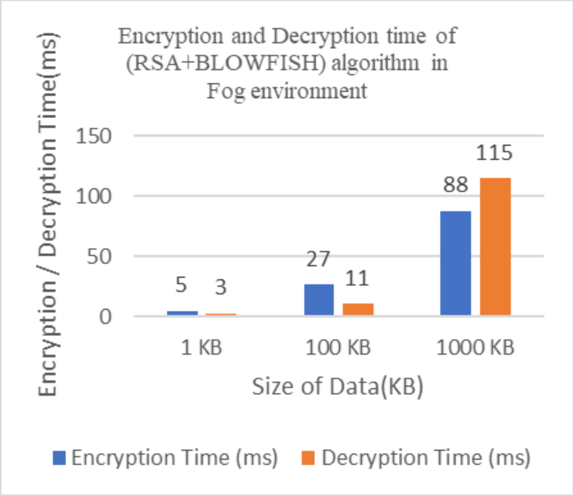

Figure 9: Encryption and Decryption Time of (RSA+BLOWFISH) algorithm in Fog environment

The throughput of the integrated encryption scheme is calculated. It is found that the integrated encryption scheme has more throughput as compared to single encryption scheme. The graph of the throughput of (RSA+BLOWFISH) algorithm is shown in Figure 10.

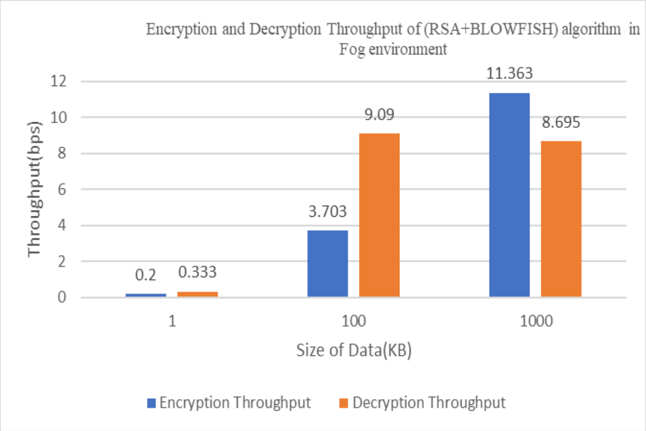

Figure 10: Encryption and Decryption Throughput of (RSA+BLOWFISH) algorithm in Fog environment

(II) Second Combination (RSA + AES) Algorithm: An integrated security scheme using the (RSA+AES) algorithm is implemented in the Fog environment to analyse the performance of the algorithm. This is a combination of the asymmetric and symmetric algorithms. The encryption and decryption time of the integrated encryption scheme is calculated on the data sizes of 1KB, 100KB, 1000KB respectively. It is found that the integrated encryption scheme has lesser encryption decryption time than single encryption algorithm. The graph of the encryption-decryption time of the (RSA+AES) algorithm is shown in Figure 11.

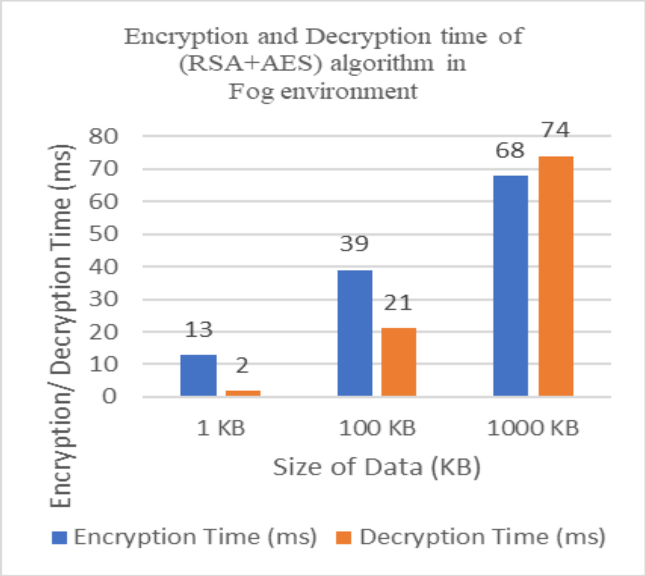

Figure 11: Encryption and Decryption Time of (RSA+AES) algorithm in Fog environment

The throughput of (RSA+AES) algorithm is shown in Figure 12. The integrated encryption scheme has more throughput than the single encryption scheme.

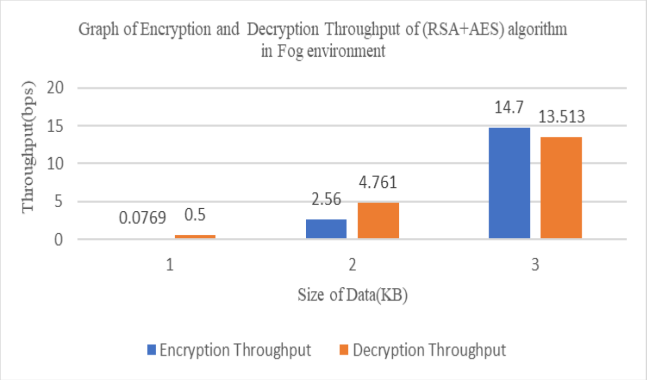

Figure 12: Encryption and Decryption Throughput of (RSA+AES) algorithm in Fog environment

EVALUATION AND DISCUSSION

(1) Evaluation in terms of Encryption-Decryption Time: The encryption-decryption time is measured in msec. Data of various sizes and types are used for encryption and decryption. It has been observed that encryption time is more than decryption time for all the data sets. A graphical representation of the encryption-decryption time of all the implemented algorithms is shown in Figure 13. It is found that the integrated encryption scheme has the least encryption decryption time among all the algorithms being applied in the Fog environment.

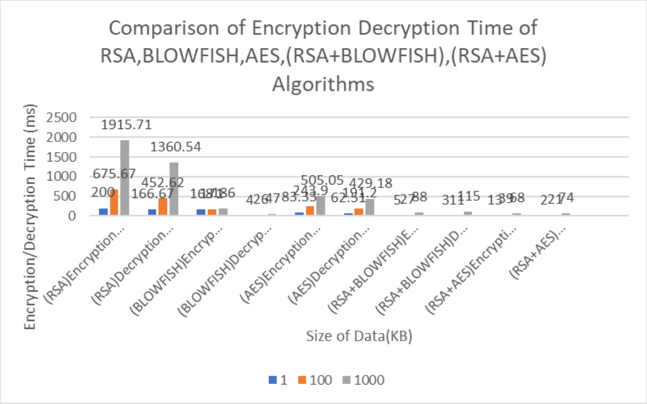

Figure 13: Graphical representation of Encryption Decryption Runtime

(2) Evaluation in terms of Throughput: The Throughput is measured in bps. Data of various sizes and types are used for encryption and decryption. The throughput is measured for all the implemented algorithms. The graph of the throughput is shown in Figure 14.

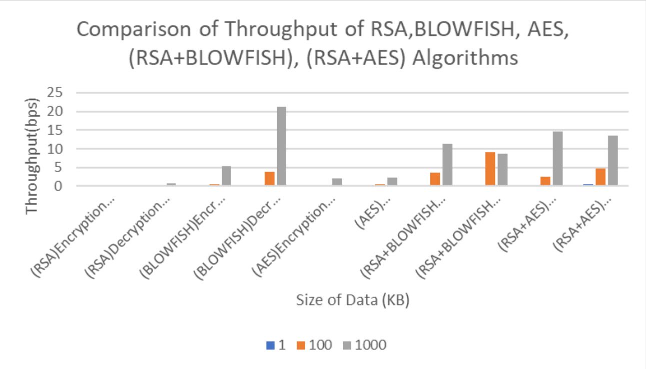

Figure 14: Graphical representation of Encryption Decryption Throughput.

CONCLUSION

E-Health is a system of providing essential health services with the help of electronic technologies. This system was started many years ago, but it gained its actual importance during the pandemic period. Electronic healthcare services generated a lot of data. The management of huge data is a concern. Cloud computing came up as a support for the processing and storage of data. But when it came to latency and bandwidth consumption, a new system of processing near the generation of data came as a Fog Computing with distributed processing, reduced delay, and less bandwidth. Here the security of sensitive data is a prime concern. Security can be achieved with a technique called cryptography. The security algorithms have been implemented in the Fog-enabled E-Healthcare System. The RSA, BLOWFISH, AES, and Integrated Encryption Scheme of (RSA+BLOWFISH) and (RSA+AES) combinations have been implemented. The comparison of the performance of RSA, BLOWFISH, AES, and the Integrated encryption scheme of (RSA+BLOWFISH) and (RSA+AES) combination security algorithm is done on the basis of key size, encryption-decryption time, and throughput to see the security as well as the performance of the system. It is found that encryption time is more than decryption time in almost every algorithm. The single-layer security has good performance as we move from asymmetric to symmetric algorithms. The BLOWFISH has the least encryption and decryption time and more throughput in a single encryption algorithm. The Integrated Encryption Scheme of (RSA+BLOWFISH) and (RSA+AES) combinations are also applied in the Fog environment. It is found that encryption decryption time decreases and throughput also increases in the Integrated Encryption Scheme. The (RSA+AES) Integrated Encryption Scheme of security algorithms have more performance than (RSA+BLOWFISH). So, to achieve the security of the E-Health system in the Fog computing environment it is more efficient to use Integrated Encryption Scheme.

REFERENCES

Ai, Yuan, Mugen Peng, and Kecheng Zhang. "Edge computing technologies for Internet of Things: a primer." Digital Communications and Networks 4, no. 2 (2018): 77-86.

Al-Khafajiy, Mohammed, Thar Baker, Atif Waraich, Dhiya Al-Jumeily, and Abir Hussain. "IoT-fog optimal workload via fog offloading." In 2018 IEEE/ACM international conference on utility and cloud computing companion (UCC companion), pp. 359-364. IEEE, 2018.

Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, Xiaoshuang Xing, and Xiuzhen Cheng. "An attribute-based encryption scheme to secure fog communications." IEEE access 5 (2017): 9131-9138.

Atlam, Hany F., Ahmed Alenezi, Abdulrahman Alharthi, Robert J. Walters, and Gary B. Wills. "Integration of cloud computing with internet of things: challenges and open issues." In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 670-675. IEEE, 2017.

Atlam, Hany F., Ahmed Alenezi, Raid Khalid Hussein, and Gary B. Wills. "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things." International Journal of Computer Network & Information Security 10, no. 1 (2018).

Atlam, Hany F., Ahmed Alenezi, Robert John Walters, and Gary B. Wills. "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things." IoTBDS 4 (2017): 254-260.

Blaze, Matt, Gerrit Bleumer, and Martin Strauss. "Divertible protocols and atomic proxy cryptography." In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 127-144. Springer, Berlin, Heidelberg, 1998.

Bonomi, Flavio, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. "Fog computing and its role in the internet of things." In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13-16. 2012.

Bonomi, Flavio, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. "Fog computing: A platform for internet of things and analytics." In Big data and internet of things: A roadmap for smart environments, pp. 169-186. Springer, Cham, 2014.

Carlos Andres Lara-Nino, Arturo Diaz-Perez, Miguel Morales-Sandoval. "Elliptic Curve Lightweight Cryptography: a Survey." IEEE Dataport, November 8, 2018. doi: https://dx.doi.org/10.21227/bqfj-6c39.

Diro, Abebe Abeshu, Naveen Chilamkurti, and Yunyoung Nam. "Analysis of lightweight encryption scheme for fog-to-things communication." IEEE Access 6 (2018): 26820-26830.

Farjana, Nishat, Shanto Roy, Md Mahi, Julkar Nayeen, and Md Whaiduzzaman. "An identity-based encryption scheme for data security in fog computing." In Proceedings of the International Joint Conference on computational intelligence, pp. 215-226. Springer, Singapore, 2020.

Giang, Nam Ky, Seonghoon Kim, Daeyoung Kim, Markus Jung, and Wolfgang Kastner. "Extending the EPCIS with Building automation systems: a new information system for the internet of things." In 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 364-369. IEEE, 2014.

Huang, Qinlong, Yixian Yang, and Licheng Wang. "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things." IEEE Access 5 (2017): 12941-12950.

Khan, Saad, Parkinson, Simon, and Qin, Yongrui. "Fog computing security: a review of current applications and security solutions." Journal of Cloud Computing: Advances, Systems and Applications, 2017.

Kulkarni S, Saha S, Hockenbury R. "Preserving privacy in sensor-fog networks." In: Internet Technology and Secured Transactions (ICITST), 2014, 9th International Conference For. IEEE, pp 96-99, 2014.

Miao, Yinbin, Jianfeng Ma, Ximeng Liu, Jian Weng, Hongwei Li, and Hui Li. "Lightweight fine-grained search over encrypted data in fog computing." IEEE Transactions on Services Computing 12, no. 5 (2018): 772-785.

Mohd, Bassam J., and Thaier Hayajneh. "Lightweight block ciphers for IoT: energy optimization and survivability techniques." IEEE Access 6 (2018): 35966-35978.

Mustacoglu, Ahmet F., Ferhat O. Catak, and Geoffrey C. Fox. "Password-based encryption approach for securing sensitive data." Security and Privacy 3, no. 5 (2020): e121.

N the Ni, Jianbing, Kuan Zhang, Xiaodong Lin, and Xuemin Shen. "Securing fog computing for internet of things applications: Challenges and solutions." IEEE Communications Surveys & Tutorials 20, no. 1 (2017): 601-628.

Patil, P. V. "Fog Computing." International Journal of Computer Applications (0975-8887), National Conference on Advancements in Alternate Energy Resources for Rural Applications (AERA-2015), 2015.

Peter, Nisha. "Fog computing and its real-time applications." Int. J. Emerg. Technol. Adv. Eng 5, no. 6 (2015): 266-269.

Pranati V. Patil’ “Fog Computing” International Journal of Computer Applications International Journal of Computer Applications (0975-8887), National conference on Advancements in Alternate Energy Resources for Rural Applications (AERA-2015), 2015.

Schumacher M, Fernandez-Bugloioni E, Hybertson D, Buschmann F, Sommerland P. Security Patterns: Integrating security and systems engineering. Wiley, 2013.

Shi, Yingjuan, Gejian Ding, Hui Wang, H. Eduardo Roman, and Si Lu. "The fog computing service for healthcare." In 2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), pp. 1-5. IEEE, 2015.

Suárez-Albela, Manuel, Tiago M. Fernández-Caramés, Paula Fraga-Lamas, and Luis Castedo. "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications." Sensors 17, no. 9 (2017): 1978.

Tsai, Kun-Lin, Fang-Yie Leu, Ilsun You, Shuo-Wen Chang, Shiung-Jie Hu, and Hoonyong Park. "Low-power AES data encryption architecture for a LoRaWAN." IEEE Access 7 (2019): 146348-146357.

Vaquero, Luis M., and Luis Rodero-Merino. "Finding your way in the fog: Towards a comprehensive definition of fog computing." ACM SIGCOMM computer communication Review 44, no. 5 (2014): 27-32.

Verma, Manisha, Neelam Bhardwaj, and Arun Kumar Yadav. "Real-time efficient scheduling algorithm for load balancing in fog computing environment." Int. J. Inf. Technol. Comput. Sci 8, no. 4 (2016): 1-10.

Wen, Zhenyu, Renyu Yang, Peter Garraghan, Tao Lin, Jie Xu, and Michael Rovatsos. "Fog orchestration for internet of things services." IEEE Internet Computing 21, no. 2 (2017): 16-24.

Yi, Shanhe, Zijiang Hao, Zhengrui Qin, and Qun Li. "Fog computing: Platform and applications." In 2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb), pp. 73-78. IEEE, 2015.

Zhang, Peng, Joseph K. Liu, F. Richard Yu, Mehdi Sookhak, Man Ho Au, and Xiapu Luo. "A survey on access control in fog computing." IEEE Communications Magazine 56, no. 2 (2018): 144-149.

Zhang, Wenjuan, and Gang Li. "An efficient and secure data transmission mechanism for Internet of vehicles considering privacy protection in fog computing environment." IEEE Access 8 (2020): 64461-64474.

Zhang, Wenjuan, and Gang Li. "An efficient and secure data transmission mechanism for Internet of vehicles considering privacy protection in fog computing environment." IEEE Access 8 (2020): 64461-64474.