Article

Not peer-reviewed version

Secure Edge Communications Over the IoT

Andreas Plageras , Christos L. Stergiou , Konstantinos Psannis [*]

Posted Date: 1 February 2024

doi: 10.20944/preprints202402.0020.v1

Keywords: Algorithms; IoT; Big Data Privacy; Cyber-Security; Edge Computing; Healthcare; Threats; Vulnerabilities

Article

Secure Edge Communications over the IoT

Andreas P. Plageras [1], Christos L. Stergiou [2] and Konstantinos E. Psannis [3]

[1] University of Macedonia, School of Information Sciences, Department of Applied Informatics; a.plageras@uom.edu.gr

[2] University of Macedonia, School of Information Sciences, Department of Applied Informatics; c.stergiou@uom.edu.gr

[3] University of Macedonia, School of Information Sciences, Department of Applied Informatics; kpsannis@uom.edu.gr

* Correspondence: kpsannis@uom.edu.gr; a.plageras@uom.edu.gr;

Abstract: The world has changed. New technologies, new trends, new protocols, new efficient algorithms, and systems have been used widely by civilized countries to have better and more convenient living. In this research, there have been introduced many new terms, technologies, and mechanisms. Moreover, threats, attacks, and vulnerabilities have been studied and a novel scenario has been proposed in order to overcome all these violations that have been presented in this paper. The scenario is based on a security model that has been proposed for critical sectors, such as hospitals, industries, etc., which need efficient solutions to go one step further and improve the secure and efficient living and treatment of people. The aim of this research has been to understand through research the IoT security issues and propose the appropriate solutions based on the most suitable security algorithms. The results, which have been based on the complexity, the throughput, the power consumption, the strength, and the memory usage of the algorithms studied, have been hopeful and helpful for future research and experimentation.

Keywords: algorithms; IoT; big data privacy; cyber-security; edge computing; healthcare; threats; vulnerabilities

1. Introduction

Cyber-crime is not different at all than regular crime that is all over the world from the past centuries. It is very important to recognize that we cannot stamp out the cyber-crime, as we cannot exterminate the typical crime.

However, there are two primary points to defend against cyber-attacks. The first point refers to the basic level of protection that companies and individuals can do in a daily basis, just like when you lock the door when you leave the house. It is important to secure the devices and the data the same way and use security principals, such as those used when protecting a person or a property. The second point refers to the deterrence. Today, there is a broad difference in laws and legislations. Many countries do not have vigorous cyber-security laws or are outdated and need to be modernized. In fact, having inclusive laws to operate as deterrent and well-read and well-trained personnel (judges, prosecutors, etc.) to persecute criminals when identified is an important aspect that plays vital role in fighting cyber-crime.

Many researchers claim that instead of using a simple password to secure data, devices, and systems there can be used modern security suites (e.g. G-suite), data loss prevention and encryption technologies, multi-factor authentication, and even, it can be done a system update on a daily basis to prevent the biggest percent of the attacks that occur.

James Dempsey (Executive director in the University of California – Berkeley Center of Law and Technology) once said in an interview: "Encryption is foundational". What that means is that there is strong, default encryption and encryption with a government access option. He also said that building in government "backdoors" or access points as they can be characterized, means that vulnerability is created at the same moment.

The security model, which is used until now, is based on notifications and acquiescence. This means that first you are asked in most of the cases a question and then you have to agree or disagree by clicking "Accept" or "Decline" respectively. But now with the "Internet of Things" (IoT) devices, services, and systems are interconnected with each other and with the Internet, resulting in massive production of data that this model cannot withstand. This is because the collection of these enormous amounts of data is due to the millions of devices used in a daily basis. [1,2]

So, new privacy and security mechanisms should be implemented that will not use the notifications and acquiescence security model, but will take into consideration the limits of data collection and usage, the individual access and control of the "Big Data", and ways that up until now just have not existed. [3,4]

"Artificial Intelligence" (AI) is a technological advance that provides various solutions to various issues, which are based on the security and privacy of data, by taking into consideration the energy consumption and the complexity of the algorithms.

To address the cyber-security threats, it is also important to make and have partnerships. This means that all information collected about security issues has to be shared in order to deploy better security mechanisms. So, it has to be a "shared responsibility" between the companies, the governments, and the citizens. [5–8]

Last but not least, new legislations have been passed and more information can be shared between companies, governments, and citizens. But, what information should be shared, what is most useful, in what context, and for who. These questions have to be answered by taking into account the impact on privacy which has to be in the lowest level.

As the amounts of data are produced by every device all over the world, there is an imperative need for data processing, data storage, data mining, data analysis, and of course data privacy. Data privacy is the most crucial issue since the beginning of the internet (20 years ago), as data production increases every day. Due to this, there have to be deployed strict rules and laws to secure the everyday amounts of data that are continuously raising fast. Such rules and laws had been introduced in the last 20 years. But 20 years ago, it was a very different era in terms of the Internet since it was not commonly used and it was not as much personally used.

Today, every European citizen has to follow the "General Data Protection Regulation" (GDPR) that came on for the "European Union" (EU). This is by far the most significant piece of European data protection enactment as Edina Bakos (Program Manager of Google Cloud) said.

All these questions will be answered in the following sections. More specifically, this research has been divided in section II, where the security and data privacy threats have been listed and some challenges and solutions have been discussed. In section III, in which a security model for each layer has been presented. In section IV, where the benefits gained by the proposed scenario have been presented and explained. Finally, in section V, in which there can be observed the conclusions of the research and some future improvements and ideas.

2. Security Threats Challenges and Solutions

As applications based on "Internet of Things" (IoT) have been used widespread in every sector, many research studies provide useful information about new trends of IoT, the issues that they cause, some solutions that already exist, and various challenges that need to be solved in order to gain the benefits of the Internet technology.

Specifically, many researchers make illustrations of the most recent affection of issues based on security mechanisms, techniques, and methods related to the technology of the IoT. One feature of IoT that has a big impact on security and privacy of information is the interdependency. This means that due to the rapid increase of devices and data, more and more automation systems have been developed to make human interaction disappear. [1]

Nowadays, many of these systems are absolutely controlled by services, platforms, and applications such as the "Google Cloud", the "IoT Platform", and the "Android Applications" respectively. To sum up, the interdependence of devices, applications, and systems could be easily damaged by the attackers to fulfill their goals. Such a trigger that an attacker could have is the network level security, which in most cases is vulnerable at attacks like these related to “Distributed Denial of Service” (DDoS) attacks.

Moreover, another feature of IoT that is critical for the security of the automation systems is the variety of protocols used by the miscellaneous devices. For example, every device itself has a processor and its own characteristics, but cannot withstand every kind of protocol or feature that is out of its capabilities. [1]

A circumstance relevant to what just mentioned is the constrained energy of the IoT devices which constitutes the next feature of IoT. Due to the fact that these devices are very tiny and very lightly built, they do not need much energy to operate. This constrained energy leads to crucial problems and in most cases to vulnerabilities, because of the restricted security mechanisms and algorithms used.

Furthermore, networks of private computers, regularly named as “botnets”, had been contaminated in the near past, with malicious software and were controlled as a group without the providers’ knowledge. An example could be a spam message that was sent through the application to the user’s device or more likely the DDoS attacks used by crackers to simulate users’ requests and achieve their goal. [1]

In the past, many researchers had proposed detection systems and methods that detect DDoS attacks in devices which use the “IPv6 over Low-power Wireless Personal Area Network” (6LoWPAN) protocol [5–8]. In Table I below, some of the most crucial threats in every IoT layer that have been studied by many scientists and some solutions can be observed. [5,6]

Table I. Crucial Threats in each IoT Layer.

Layers	Threats, Attacks, Vulnerabilities	Solutions
Physical and Abstraction Layer	Unauthorized access to topics Tracking Denial of Service Repudiation Spoofing Packet Manipulation Eavesdropping DoS Exhaustion Unfairness Sybil	Authentication Knowledge security (RSA, DSA, Blowfish, DES, 3DES, etc) Access Control (Digital Signatures, MAC)
Network and Transportation Layer	Unauthorized access Sybil attack Depression attack Sleep deprivation attack DoS Code injection attack Man-in-the-Middle attack	Authentication Secure Routing Knowledge Security Intrusion Detection Risk Management Risk Assessment
Application and Presentation Layer	Code injection attack DoS Spear-phishing attack Sniffing attack	Authentication Secure Routing Knowledge Security Intrusion Detection

	Risk Management Risk Assessment

The security mechanisms have to be updated and become even more adaptable to the changes that are coming together with the advances in technologies and the fifth generation of cellular networks (5G). The 5G connectivity will bring new critical issues in security [1,4].

In Table II below, the solutions for attacks that have been recorded in IoT environments have been presented and could be integrated in the proposed model.

Table II. Solutions for Attacks & Problems in IoT Environments.

Ref.	Attacks	Solutions
[1]	IoT botnets	1) Fuzzy rule interpolation (FRI) for detection, 2) Logistic regression which allows probability estimation, 3) Machine Learning techniques for IoT security threats detection 4) Auto-encoders 5) Adaptive filters
[4]	Physically dynamic tracing attack	Pseudonyms technique – hiding location and user identity,
	Node compromise attack and Target-oriented compromise attack	1) Authentication of users and devices/nodes, 2) Cloud-based IoT DTNs (Delay-Tolerant Networks) - credit-based incentive mechanism
	Injection attack	Avoid replication of victim node
	Layer adding attack Layer removing attack	Secure outsourced data aggregation without public key homomorphic encryption
[6]	Remote attack	Secure the area and devices
	Modification	Collision-free one-way hash function to guarantee the integrity of the message transmission
	Eavesdropping	Securing Key exchange process
[8]	DDoS attack	1) Fuzzy rule interpolation (FRI) for detection, 2) Logistic regression which allows probability estimation, 3) Machine Learning techniques for IoT security threats detection 4) Auto-encoders 5) Adaptive filters 6) Lightweight agents – Blockchain smart contract
	Man in the middle attack	Non-SSL and Secure connection SSL approaches
	Proximity-based attack	When combining large RSS-variation and

		matching between RSS-trace and smartphone sensor-trace to reliably detect and authenticate
[16]	Interception problem	Encryption of data
	Spoofing problem	Message Authentication Codes (M.A.C.) & Digital Signature
	Falsification problem	Message Authentication Codes (M.A.C.) & Digital Signature
	Repudiation problem	Digital Signature

3. Comparative Analysis of Security Algorithms

The security algorithms mostly used in IoT environments are the symmetric and asymmetric encryption algorithms. [9–11]

Block ciphers and stream ciphers are two encryption approaches related to the symmetric key cipher. They are applied in order to transform the plain text into cipher text. The main variation between them is that the former conducts the conversion through taking the block of plain text at once, while the latter conducts the conversion through processing 1 byte of plain text during each iteration. [12–15]

For the encryption and decryption in symmetric cryptography an identical key is used for both methods. Due to a comparative analysis of such algorithms used in IoT environments, some of the most known and used algorithms include AES (Advanced Encryption Standard), Blowfish, 3DES (Data Encryption Standard), Serpent, and Twofish. Symmetric algorithms are extensively used in data transmission and storage. However, it is not always easy or possible to share one secret key. [16–19]

Asymmetric encryption is also known as public key cryptography. Its objective is to bypass the need to share one secret. The main idea behind this approach is to use different keys in encryption and decryption. Its base lies on problems that the designer thinks that are not solved fast such as prime factorization, discrete Logarithm, and elliptic curves. After comparing such algorithms, the most known algorithms include ECDH (Elliptic-curve Diffie–Hellman), ECDSA (Elliptic Curve Digital Signature Algorithm), RSA (Rivest–Shamir–Adleman), El-Gamal, and SRP (Secure Remote Password). This type of encryption achieves data confidentiality (during the encryption phase), data integrity and authenticity (signatures) or key exchange over insecure channels. [18,20,21]

One common example of asymmetric encryption is the exchange of a message between Alice and Bob. Alice and Bob generate a pair of keys (public and private). The public key has been published over the internet. The encryption of the message has been performed using the public key of Bob by Alice, and transmits it to Bob. The decryption of the message has been performed by Bob using his private key in order to decrypt the messages that have been encrypted through the public key. Also, Alice uses her private key in order to sign a message, and transmit it to Bob. Bob verifies the integrity and authenticity of this message, since he knows the public key of Alice.

Moreover, the problem of a number factorization has gained significant attention in modern cryptography as several cryptographic protocols base their safety in the difficulty of solving it (with the most known and applied the RSA). The RSA cryptosystem was proposed by Rivest, Shamir and Adleman and is the first public key-based cryptosystem. [18]

Furthermore, Chaotic encryption is based on the mathematic chaos theory. Some of its main applications are image encryption, aimed at improving the security of digital images, generation of hash functions, and generation of random numbers. There are both symmetric and asymmetric chaotic cryptographic algorithms, however the majority of the relevant approaches falls under the asymmetric group. Furthermore, discrete chaotic maps are commonly used in relevant applications.

AES has been proven robust against all major security attacks. Its cipher key is consisted of at least 128 bits, which provides 2128 possible keys. Hence, the conduction of brute force attack is impractical. Furthermore, this algorithm applies an S-box substitution table that is retrieved through the determination of the multiplicative inverse for a given number in Galois field, being capable of resisting both linear and differential cryptanalysis. However, it is vulnerable to timing attack, since the applied sequence of S-box lookups takes variable time and depends to the key. [17,21]

On the other hand, RSA is vulnerable to brute force attack, since it applies a short secret key. Furthermore, RSA can be broken under mathematical attacks that exploit the mathematical properties of the algorithm, based on prime factors. Increasing the length of key is considered as a countermeasure against this vulnerability. An acceptable size of modulus is 2048 bits. [18,21]

Furthermore, RSA is vulnerable to timing attack, since the attacker is able to exploit the timing variation of the modular exponentiation or determine d through the necessary time for the computation of Cd(modn) for a cipher text C. There are several counteractions about these vulnerabilities (a constant exponentiation time for all exponentiations, a random delay to the exponentiation or the multiplication of the cipher text with a random number. [18,21]

Finally, another vulnerability of RSA lies to the chosen ciphertext attack. The product of two cipher texts is equal to the encryption of the product of the respective plaintexts, setting easy for an attacker to conduct a relevant attack. This issue can be resolved through padding a random number to the plaintext.

As for speed, AES provides higher speed, albeit this feature is decreased when using constant time in order to resolve the vulnerability of timing attack. On the other hand, RSA is more functional. Therefore, a combination of the two algorithms is the most suitable approach. RSA, based on asymmetric cryptography, can be used to authenticate the parties and agree on a key for a symmetric system. Then, AES, based on the symmetric approach, can be applied for large data blocks in order to take advantage of its higher speed.

Blowfish is a 64-bit block cipher with a variable-length key algorithm invented by Bruce Schneider in 1993 to replace the DES (Data Encryption Standard). Blowfish also separates a message into 64-bit chunks of equal length. A key-expansion part and a data-encryption part make up the algorithm. Blowfish is faster than DES in terms of encryption time, however, the algorithm's weak point is its weak key. There is currently no cryptographic attack capable of breaking the Blowfish algorithm in an acceptable amount of time. It's possible that a successful attack was made possible by system errors. Blowfish isn't patented and doesn't require a license, thus anyone can use it. CAST (Carlisle Adams & Stafford Tvares) uses a 128- or 256-bit key format and is like the DES algorithm. [17]

The Twofish algorithm is a symmetrical block technique with a block size of 128 bits and a key size of 256 bits in cryptography. This algorithm is related to the Blowfish algorithm that came before it. The pre-calculated key-dependent S-blocks and the complicated encryption technique are the two fundamental features of the Twofish algorithm. One-half of the encryption n-bit keys is used as the encryption key, while the other half is utilized to modify the algorithm. [17]

The architecture of the Twofish algorithm is quite similar to the Blowfish method. In terms of speed, Twofish may overtake AES. On many types of CPUs and in hardware, Twofish is quick and adaptable. Twofish can be utilized in network applications where keys are regularly updated, as well as in situations where RAM and ROM are limited. [17]

The blowfish algorithm's strengths are its speed and efficiency, as well as its ability to generate big keys with high levels of security. The Blowfish Algorithm is capable of constructing and developing a greater and larger length that ensures system security by boosting the speed of data processing by computer systems. [17,21]

Vernam's One-Time Pad is a stream cipher that functions by applying the boolean operation XOR (as described in 1st semester's "Introduction to Computer Science") to the plaintext. It offers "perfect secrecy" but is otherwise impractical when one needs to encrypt large streams of data.

Data Encryption Standard (DES). One of the oldest block ciphers (since 1977), which was used by governments, banks and finance companies. It uses a 56-bit key to encrypt 64-bit blocks of data in 16 rounds, by applying mathematical permutations, substitutions and other functions. DES is not in use any more, due to its low security.

An advanced version of it is 3DES ("triple DES"), which is technically DES applied three times to each data block. This process renders it more secure, although slower than DES, which has contributed to 3DES being used until today.

4. Proposed Security Model for each Layer

The security model has been proposed for critical sectors, such as healthcare, transportation, industries, etc., which need efficient solutions to go one step further and improve living and production. The proposed secure communication model can be observed in the following Figure 1.

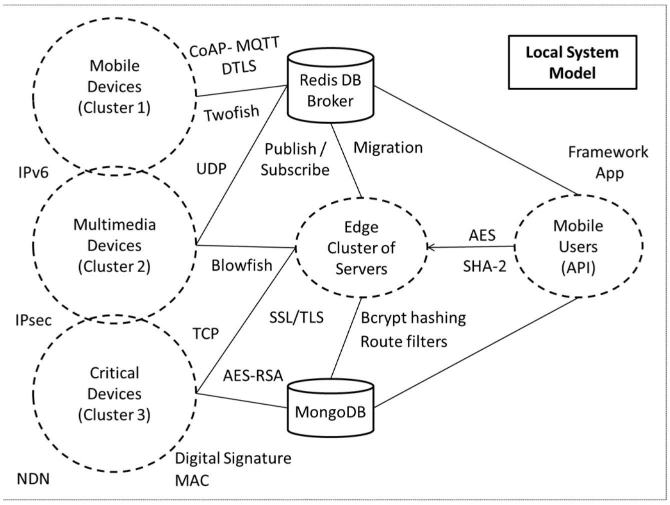


Figure 1. The proposed secure communication model.

In order to successfully attach the proposed architecture in the power and memory constrained IoT devices several metrics have been considered. Such metrics that must be measured and taken into consideration have been the complexity, the throughput of encryption and decryption, the energy consumption, and the memory needed by the devices. All these have been analyzed in the next section comprehensively in order to provide a better insight for future implementations.

To begin with the first layer (Physical-Abstraction Layer), many challenges and issues that need a solution have been addressed by various researchers. In this layer, the hardware components must first of all be protected by strict security rules and equipment (such as cameras and sensing devices) in order to ensure their safety from inside and outside the facilities. So, a solution to that problem could be given by AI and machine learning algorithms that will ensure that everybody inside and nearby the facility will be monitored and identified [9–11].

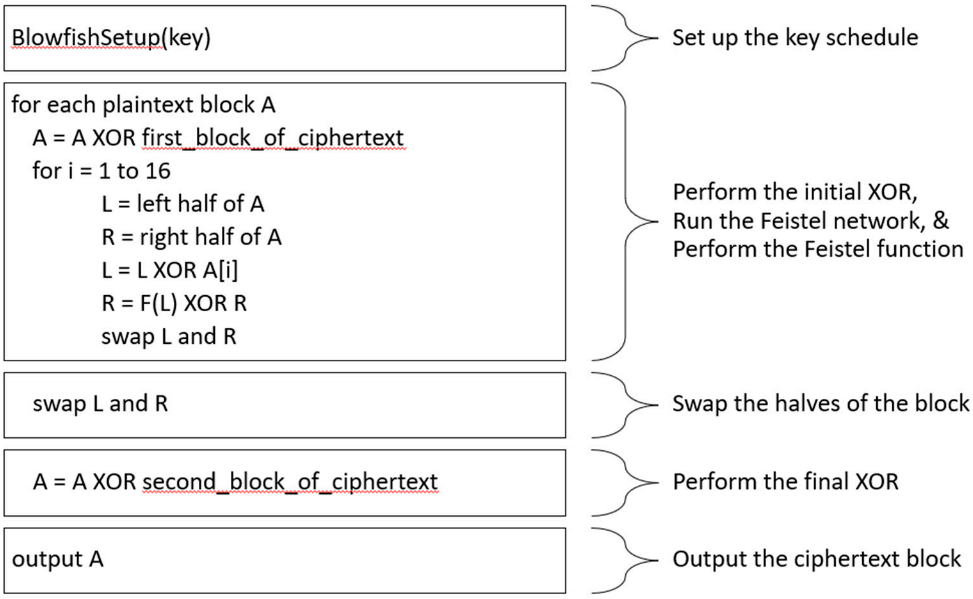
The identification can work in conjunction with a police database table, which will inform with a simple notification message both the facility's security-staff and the nearest police department. Firstly, an image will be captured using surveillance equipment (Depth Cameras) and then this image could be compared with the images stored in a database, in order to measure the similarity through an efficient probabilistic model. Thereafter, a machine learning scenario takes action. This model, while violation cannot be possible on the personal data of pedestrians, will detect specific face features and gestures. The use motion sensors that detect pedestrians' distance from a selected safe point and enables the nearest camera devices when needed. The detection of suspicious motions could be performed with the use of the relevant deep learning algorithms.

The second layer is the middleware, where the edge servers and the databases have been established. In this layer, the networking of the devices has been done by communicating with the first layer. Then, the networking of the users has been done by communicating with the application layer. Each device has been communicating with a specific cluster of servers, where load balancing and task offloading algorithms and techniques have been performed, depending on the criticalness of each device. In this layer, AI and deep learning algorithms could be used for the sensitive, complex, and important actions.

The databases that could be possibly used in the middle layer are the Redis and the MongoDB. Redis supports "Transport Layer Security" (TLS) and allows access to the topics only by authorized and authenticated users. It also provides a protected mode, in which communicates with queries from the loopback interfaces, and sends an error message to clients connecting from other addresses. Injection is not possible under normal circumstances by using a normal client library. The protocol is binary safe and is using prefixed-length strings.

The third layer is the application-presentation layer, where the application lives and the presentation of the data has been performed. First of all, the mobile users should have rich or sufficient authentication mechanisms, secured accounts, access control mechanisms, strong encryption methods etc. These mechanisms have been provided by the framework that has been used for the development of the MVC (Model-View-Controller) client architecture.

The implementation of all aforementioned security algorithms has been done using the Java, C++, JavaScript, and Python languages, but could be implemented the same way in all languages. In Figure 2 below, has been presented the use of the Blowfish security algorithm.



```
BlowfishSetup(key)

for each plaintext block A
  A = A XOR first_block_of_ciphertext
  for i = 1 to 16
        L = left half of A
        R = right half of A
        L = L XOR A[i]
        R = F(L) XOR R
        swap L and R

  swap L and R

  A = A XOR second_block_of_ciphertext

output A
```

Set up the key schedule
Perform the initial XOR,
Run the Feistel network, &
Perform the Feistel function
Swap the halves of the block
Perform the final XOR
Output the ciphertext block

Figure 2. Implemented Blowfish Security Algorithm.

5. Results

This section provides a performance analysis based on different security aspects. As it has been assumed by many researchers the performance of block ciphers is related to block and key size. The larger the block size is, the fastest the algorithm is. This is because big amounts of data will be encrypted in only one execution cycle. Likewise, the smaller the block is, more execution cycles will be needed and thus, total execution time will be increased. If the key size is very large, this will have negative consequences (slows down) in the performance of the security algorithm, although it enhances the security.

In the following Table III, a comparative analysis of the most known and used algorithms has been done and presented. The table is based on the comparative analysis section.

Therefore, the outcomes from the table below show that the AES, Blowfish, Twofish, IDEA, and TEA security algorithms are advantageous in terms of security, performance, speed, complexity, flexibility, and efficiency. Thus, it has been considered that each algorithm suites different in each IoT use case. So, a combination of the best suited algorithms will provide better and faster security, flexibility, and efficiency in each IoT layer.

In order to make the selection easier, a comparative analysis of the complexity of the two types of ciphers has been provided. The results, which can be observed in Figure 3, show that the block ciphers are the best choice for the constrained IoT devices.

Table III. Comparative Analysis of Modern Security Algorithms.

Ref	Algorithm	Cipher Type	Block Size	Key Length	Round(s)	Speed	Security	Disadvantage	Use cases
[17] [20] [21] [23]	AES	Symmetric – Block Cipher	128, 192, 256 bits	128, 192, 256 bits	10, 12, 14	Very Fast	Excellent – widely used	Vulnerable in Timing Attacks	Wi-Fi, processor, websites, mobile apps, VPN
[18] [20] [21] [24]	RSA	Asymmetric – Block Cipher	Variable	768, 1024, 2048, 4096 bits and more	1	Slow but more functional	Excellent	Vulnerable in Brute Force Attack, Timing Attack, Mathematical Attack, and Chosen Ciphertext Attack	Number Factorization, used in IoT apps, commonly found in SSL/TLS certifications, email encryption, and cryptocurrencies.
[21]	DES	Symmetric – Stream Cipher	64 bits	56 bits	16	Moderate	Insecure – out of use	Low encryption key length, susceptible to brute-force attacks	Financing, Government, Banks
[21]	3DES	Symmetric – Block Cipher	64 bits	168 (3*56) bits	48 (3*16)	Slower than DES since it is applied 3 times	Vulnerable –due to be replaced	will be phased out as an IoT encryption method by 2023	Financing, TLS protocol, Microsoft Office, Firefox, and in payment systems
[16] [17]	Twofish	Symmetric	128 bits	256 bits	16	Overtakes	More secure	Slow	Network apps and

						AES, Quick and Adaptable	but slower		Situations with limited RAM & ROM, password security and generation, and encryption of files
[16] [21]	Blowfish	Symmetric – Block Cipher	64 bits	Variable Length (32 to 448 bits)	16	Fast	Excellent	Weak key	Payments & protection of passwords, secure shell, secure telephony, OS, file and disk encryption, backups, encryption libraries and toolkits, and database security
[20]	Rijndael (AES)	Symmetric	128 bits	128, 192, 256 bits		Very fast	Excellent	-	Wi-Fi, processor, websites, mobile apps, VPN
[16] [20]	Serpent (AES)	Symmetric	128 bits	128, 192, 256 bits	32	Very fast	Excellent	-	Wi-Fi, processor, websites,

							mobile apps, VPN
[16] [20] [22]	ECDH	Asymmetric	Variable (250 bits)	Slow	Excellent	-	End-to-end encryption and post-compromise security
[16] [20] [22]	ECDSA	Asymmetric	Public key: twice the size of the security level, in bits. Private key: 1024bits	Slow	Excellent	difficulty of implementation, design flaws which reduce security in insufficiently defensive implementations	Bitcoin transactions
[24]	El Gamal	Asymmetric	768, 1024, 2048, 4096 bits and more	Slow	Depends	not secure under chosen ciphertext attack	Hybrid cryptosystems
-	SRP	Asymmetric	Large private key shared	Faster than Diffie-Hellman	More secure than SSH	-	
-	DSA	Asymmetric	Signature consists of two 160 bits numbers generated from msg and private key	Slower than RSA in encryption and signing but faster in decry	Equal in strength to RSA	-	Enables IoT products to comply with government security protocols

						ption and verification			
[20]	IDEA	Symmetric Block Cipher	64 bits	128 bits	8	Very fast in encryption time	Excellent	Weak keys	Constrained Devices
[16] [19] [20] [24]	TEA	Symmetric Block Cipher	64 bits	128 bits	Variable Suggested 64 rounds	Fast	Bad as cryptographic hash function	Suffers from equivalent keys, susceptible to a related key attack	Constrained Devices

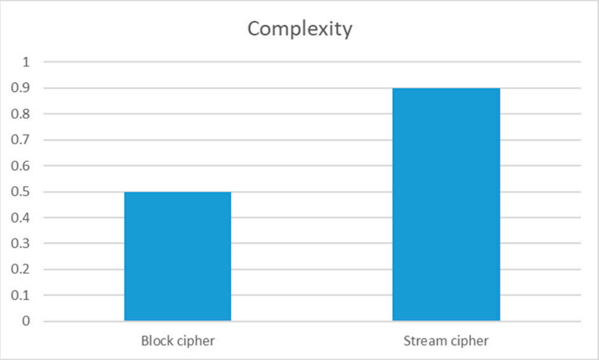


Figure 3. Comparing the complexity of block and stream ciphers.

In Figure 4 below, the results from the comparative analysis of AES and RSA security based on the key length have been provided.

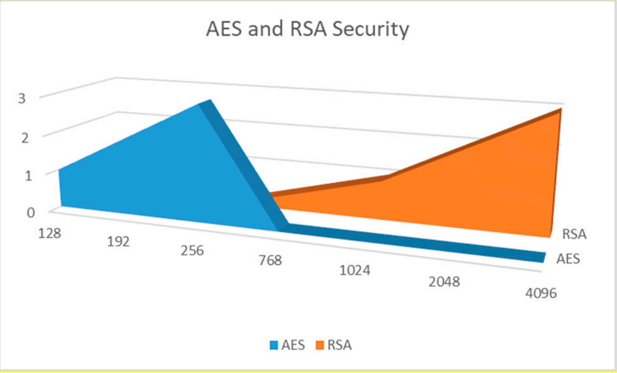


Figure 4. Comparative analysis of AES and RSA security.

In Figure 5 below, the results from the comparative analysis of security algorithms based on the equation of encryption throughput below have been provided.

$$Encryption\ Throughput = \frac{Bytes\ of\ PlainText}{Encryption\ Time} \quad (1)$$

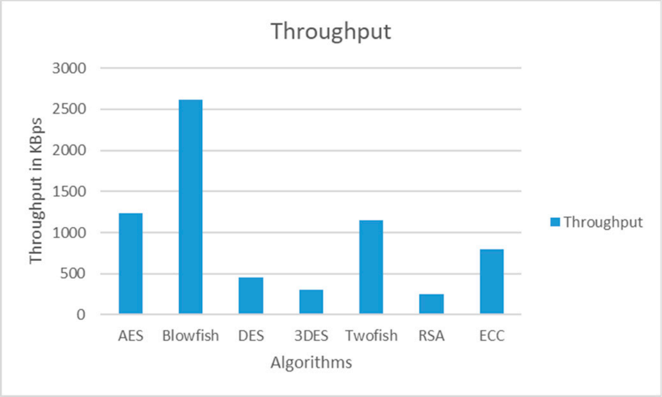


Figure 5. Comparing security algorithms based on throughput.

The energy consumption has been measured using the following equation 2:

$$Energy\ Consumption = Voltage * ElecVol * CCyc * T \qquad (2)$$

where, ElecVol is the electricity volume, CCyc is the number of clock cycles, and T the period.

The following Figure 6 shows the energy consumption measured with the use of the above equation 2 for each of the compared algorithms. [24]

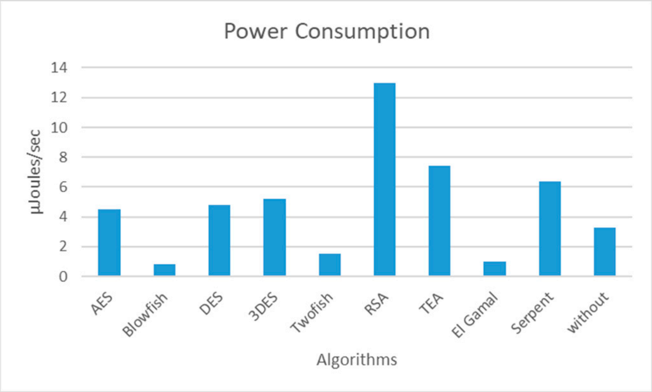


Figure 6. Energy Consumption of Security Algorithms.

An algorithm's strength is based on the size of the key. So, from Table III above, the following Figure 7 has been constructed.

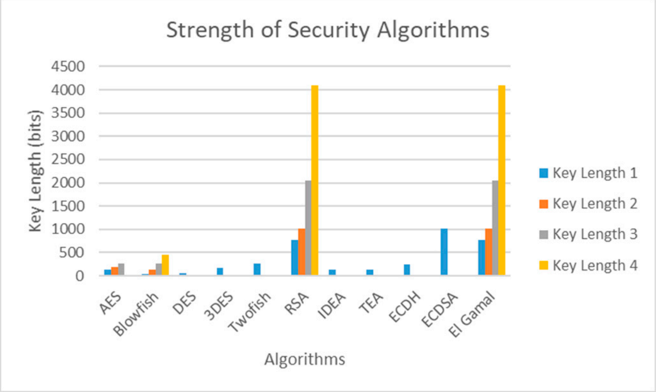


Figure 7. Algorithms' strength based on the key size.

To start with the basic security problems, there have been listed the interception problem, the spoofing problem, the falsification problem, and the repudiation problem. The solution for the interception problem is the encryption of data. The solutions for the spoofing and falsification problems are the "Message Authentication Codes" (M.A.C.) and the "Digital Signature". Finally, the solution for the repudiation problem is again the "Digital Signature". A very commonly used security algorithm is SHA-2 which has been widely used. This algorithm is based on "Hash Functions".

Confidentiality and data integrity have also been guaranteed since each device and user has been authenticated. The hash class provided by the framework for the authentication is based on "Bcrypt hashing" (Password-Hashing function based on Blowfish cipher) and the "Auth::attempt" method. "Route filters" could also be added to give access in a specified route only to authenticated users. The framework also provides CSRF (Cross-Site Request Forgery) protection and gives a solution to the cross-site request forgeries by just using a single method. AES encryption has also been provided by the framework.

Last but not least, the hybrid security mechanism can provide in conjunction with the framework API a more secure and efficient environment for patients and hospitals or for any industry. A data learning solution then can extend the smart actions that the system will take in order to become stronger.

6. Conclusions

In this paper have been proposed useful ideas about the security and the privacy of the large-scale data provided by billions of devices in critical sectors (such as hospitals) around the world. In this paper, the threats, the most common attacks, and the security algorithms that exist nowadays and used in the IoT era have been discussed.

To overcome all violations, a secure and efficient communication model has been proposed. The proposed scenario is based on an efficient communication model that improves security in critical sectors like hospitals and industries, which need efficient solutions to go one step further and improve the safety of people, production lines and devices, and eventually buildings.

A comprehensive study of the most used security algorithms has been also done. Specifically, this paper provides a comparative study based on the complexity, the throughput, the power consumption, the strength, and the memory usage of the algorithms studied. The experimental results seem to be helpful for IoT security and suggest a hybrid solution since each algorithm treats specific situations in every system's layer.

In the future, similar scenarios, such as the proposed, need to be implemented, not only for hospitals, companies, and governments, but also, inside organizations, systems, networks, and so on. A data learning solution then can extend the actions that the system will take in order to become stronger and smarter.

References

1. Wei Zhou, Yuqing Zhang, and Peng Liu. "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE Internet of Things Journal, 15 June 2018.
2. Anass Sedrati and Abdellatif Mezrioui, "A Survey of Security Challenges in Internet of Things", Advances in Science, Technology and Engineering Systems Journal (ASTES), Vol. 3, No. 1, pages: 274-280, 2018.
3. Wencheng Sun, Zhiping Cai, Yangyang Li, Fang Liu, Shengqun Fang, and Guoyan Wang, "Security and Privacy in the Medical Internet of Things: A Review", Security and Communication Networks, Hindawi, Volume 2018, Article ID 5978636, 9 pages, 2018.
4. Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions", IEEE Communication Magazine, January 2017.
5. Charles Wheelus and Xingquan Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework", MDPI, IoT Journal, 259-285, October 2020.
6. Fahad Mira, "IoT security threats analysis based on components, layers and devices", American Journal of Science and Engineering (AJSE) 2019, Vol. 1, Issue 1, 1-10.

7. Rachit, Shobha Bhatt, and Prakash Rao Ragiri, "Security Trends in Internet of Things: a survey", Springer Nature Jurnal, Applied Sciences, (2021), 3:121.
8. Wissam Abbass, Zineb Bakraouy, Amine Baina, and Mostafa Bellafkih, "Classifying IoT security risks using Deep Learning algorithms", IEEE, 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 16-19 Oct. 2018.
9. Lin Shi, Shah Nazir, Liquan Chen, and Rui Zhu, "Secure convergence of artificial intelligence and internet of things for cryptographic cipher-a decision support system", Springer, Multimedia Tools and Applications (2021) 80:31451-31463.
10. Zhihan Lv and Liang Qiao, "AI-empowered IoT Security for Smart Cities", ACM Transactions on Internet Technology, Vol. 21, No. 4, Article 99, July 2021.
11. Taher M. Ghazal, "Internet of Things with Artificial Intelligence for Health Care Security", Springer, Arabian Journal for Science and Engineering, Research Article, Special Issue on Frontiers in Parallel Programming Models for Fog and Edge Computing Infrastructures, August 2021.
12. Qing Fan, Jianhua Chen, Lazarus Jegatha Deborah, and Min Luo, "A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain", Elsevier, Journal of Systems Architecture 117 (2021) 102112.
13. Khalid Haseeb, Ikram Ud Din, Ahmad Almogren, Imran Ahmed, and Mohsen Guizani, "Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things", Elsevier, Sustainable Cities and Society Journal, 68 (2021) 102779.
14. Maha Alqallaf, "Towards a Safe and Secure Internet of Things Critical Infrastructure", International Journal of Computer Science and Information Security (IJCSIS), Vol. 19, No. 2, February 2021.
15. Shancang Li, Shanshan Zhao, Geyong Min, Lianyong Qi, and Gang Liu, "Lightweight Privacy-Preserving Scheme using Homographic Encryption in Industrial Internet of Things", IEEE Internet of Things Journal, 2327-4662, 2021.
16. Nuzhat Khan, Nazmus Sakib, Ismot Jerin, Shaela Quader, and Amitabha Chakrabarty, "Performance Analysis of Security Algorithms for IoT devices", 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 21-23 Dec 2017, Dhaka, Bangladesh.
17. Dr. Sam Rizvi, Dr. Syed Zeeshan Hussain, and Neeta Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes", IEEE, 2011 International Conference on Communication Systems and Network Technologies.
18. Rana M Pir, "Security improvement and Speed Monitoring of RSA Algorithm", International Journal of Engineering Development and Research (IJEDR), Volume 4, Issue 1, 2016.
19. Zeesha Mishra and Bibhudendra Acharya, "High throughput novel architectures of TEA family for high speed IoT and RFID applications", Journal of Information Security and Applications, 61 (2021).
20. Baraa Mohammed Hassan and Haider K. Hoomod, "Comparative Study of Encryption Algorithms for Data Security in WoT and IoT", Turkish Journal of Computer and Mathematics Education, Vol. 12, No. 12, pp 2722-2727, 2021.
21. Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham, and Mohamed Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", Symbiosis, Journal of Computer Science Applications and Information Technology, 2018.
22. Naveen Kolhe and Nikhat Raza, "Throughput Comparison Results of Proposed Algorithm with Existing Algorithm", The International Journal of Engineering and Science (IJES), Vol. 2, Issue 12, pp 92-98, 2013.
23. Ljubomir M. Vracar, Milan D. Stojanovic, Aleksandar S. Stanimirovic, and Zoran D. Prijic, "Influence of Encryption Algorithms on Power Consumption in Energy Harvesting Systems", Hindawi, Journal of Sensors, Volume 2019.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.