AIP Conference Proceedings

RESEARCH ARTICLE | APRIL 02 2019

Cross-object information security: A study on new generation encryption FREE

Onder Sahinaslan ✉; Ender Sahinaslan

AIP Conf. Proc. 2086, 030034 (2019)
https://doi.org/10.1063/1.5095119

View Online Export Citation

Articles You May Be Interested In

Cryptographic methods and development stages used throughout history
AIP Conf. Proc. (April 2019)

Encryption protocols on wireless IoT tools
AIP Conf. Proc. (April 2019)

On the internet of things: Security, threat and control
AIP Conf. Proc. (April 2019)

11 July 2025 11:02:33

AIP Publishing

Cross-Object Information Security: A Study on New Generation Encryption

Onder Sahinaslan[1, a)] and Ender Sahinaslan[2, b)]

[1]*Maltepe University, Information Technology, Istanbul, Turkey*
[2]*Information Technology Adviser, Istanbul, Turkey*

[a)] Corresponding author: ondersahinaslan@maltepe.edu.tr
[b)] dr.endsa@gmail.com

Abstract. Research in the Internet of Things (IoT) is increasing the studies in security and privacy aspects. IoT applications is expected to have difficulties in security and privacy issues in the near future. Speed improvement of quantum computers threatens the crypto algorithms used. Strong Mathematics encryption algorithms in today's world can cause weaknesses later. They can be solved by the computers which have large enough transaction volume in the labs. Changes in technology require the change in approaches to security solutions. Smart objects can be managed over the network, including critical applications. The basis of security on data lies in the science of cryptography. Privacy and fidelity of data collected over IoT and its accurate transmission are very important. This study provides an approach on reliability of next-generation encryption algorithm in the context of objects' relativity.

Keywords: Blockchain, Cryptography, Cyber-attacks, Information Security, The Internet of things (IoT)
Mathematics subject classification: 11T71, 14G50, 94A60

11 July 2025 11:02:33

INTRODUCTION

There are many developments such as the Internet of things (IoT), cross-machine communication (M2M), artificial intelligence, quantum computers, block chain technology. Cloud computing, virtual applications, centralization of the database, the processing of large data is used commonly. How much can we trust the validity of information which is collected and transmitted from inanimate objects we use at home, at work, in the car or in many different areas[1] All these developments bring with it a number of information security problems. Technology cannot be built on unreliable information. Information must be protected under all circumstances[2]. Especially the integrity of the transmitted information should be provided. Unwanted contacts should not be able to access the encrypted data[3]. A powerful encryption substructure makes protection of top-secret data possible from organized crime organizations and cyber wars between the states. In e-transformation projects that provide cost and efficiency advantages to enterprises, a number of mistakes especially not giving special importance to personal data can cause big material losses and loss of reputation [4]. At the same time, it is an important tool for homeland security, protection of trade secrets and personal information. Nowadays, we are witnessing technological developments at the dizzying rate which are constantly evolving and touching every aspect of life. IoT constitutes an important part of the management of large data. Human-machine interaction that facilitates the everyday life is expanding the cyber network even further. According to Gartner strategic technology report in 2017 'With an estimated 21 billion connected sensors and endpoints by 2020, digital twins will exist for billions of things in the near future [5]. People since the use of the written communication have been constantly on the quest for secure communication tools. As the methods of encryption used is decrypted in time, people have looked for new methods and tools. This lookout for digital information security will continue in the future as well [6]. Cryptology is an encryption science which covers Mathematics and computer subjects. The common method used to decrypt is to replace a word or phrase with another word, number or symbol. The secrecy is preserved with digital bits which are encoded with various combinations. Research increasingly continues on new generation of block cipher algorithms.

International Conference of Mathematical Sciences (ICMS 2018)
AIP Conf. Proc. 2086, 030034-1–030034-4; https://doi.org/10.1063/1.5095119
Published by AIP Publishing. 978-0-7354-1816-5/$30.00

THE INTERNET OF THINGS (IOT) AND IMPORTANCE OF SAFETY

The Internet of things (IoT) (also referred as Internet of objects or industrial internet) is a paradigm of new technology that a machine or device network can interact with each other. IoT is recognized as one of the most important future technology areas and is followed with great interest by many industries [7]. It is used in many applications in the industry because of the demand for the smart and mobile devices. Backed by a new generation of powerful network connections these remotely managed devices are used in many applications with innovative business models [8]. When analyzed in terms of business management objectives using these technologies, it is essential that these resources are effectively and efficiently operated in compliance with business and user objectives.

Great data in terms of security and privacy-sensitiveness are kept in critical infrastructures. These systems are becoming more attractive by attackers and hackers. The cyber-attacks to IoT systems are extremely important since they can cause physical damage or even threaten human life. The complexity of these systems and the potential effect of the cyber-attacks bring with them new threats. To prevent damages from these threats in other words to provide IoT security we require many security measures. In the IoT cyber universe the physical safety of objects is as important an area as the safety of the giant network and network communication system created by these objects. Information is carried over these networks between objects. It is important to ensure the safety of information in messages which carries personal details like sender, receiver, and user password. Providing confidentiality, integrity and security of accessibility is the basis of information security. A new generation of security solutions and measures should be taken against cyber threats around us [9]. To provide security, cryptography (science of mathematical methods for the encryption of the information) is concerned with four main topics. They are; the prevention of disclosure of info by unwanted persons (privacy), the accuracy in transportation of info (integrity), the concealment of the sender ID (undeniable), and the confirmation of the receiver and the sender IDs (identification). So we use cryptology to send and receive info in a secure, consistent and confidential way.

ENCRYPTION ALGORITHMS

Cryptology is the science of the passwords. It is encrypting various messages or writings in a particular system, sending them to the recipient in a secure environment and deciphering the message. It includes intense math, algorithms and system design. By using secret key encryption structure, information is concealed with a meaningless image. Secret keys must be passed over to the receiver via a secure channel [10].

Verification and auditing are as important as the privacy. When we add our name to a message over the network and send it we prove our identity with a digital signature. Technically, digital signature is the info with a summary of the document (hash) attached to the electronic message. Any changes to the content makes hash invalid. Keys used to encrypt data is based on the properties of symmetric, asymmetric and hybrid encryption algorithms. The key size is small in the symmetric encryption. However, it is difficult to send the key securely to the receiver. In addition, math calculation algorithm is simple so usage in electronic devices are fast. Widely used symmetric algorithms are; AES (Advanced Encryption Standard), DES (Data Encryption Standard), Triple DES (3DES), MD5 (Message Digest Algorithm 5), SHA (Secure Hash Algorithm). In asymmetric encryption, public key is used for the encryption of the text, private key is used for the decryption. Very large prime numbers are used as the encryption algorithm. Asymmetric passwords are more complicated than symmetric encryption. There is no problem of sending the key to the recipient here.

On the other hand, it runs slower in electronic devices. Asymmetric algorithms are RSA (Ronald L. Rivest, Shamir and Leonard Adleman), DSA (Digital Signature Algorithm), Diffie Helman, Elliptic Curve Algorithm (ECC). Symmetric and asymmetric encryption algorithms can be used together in a hybrid structure which enables the users with fast and secure data encryption. In this way, although to a large extent the data is hidden, the basic principle behind is that the mathematical problems take such a long time to solve it. In the future, new computers equipped with superior computational capabilities will be used. Encryption algorithms when used alone will generate serious weaknesses and threats [11].

11 July 2025 11:02:33

NEW GENERATION BLOCK ENCRYPTION

Block encryption algorithms, hash chain structure, digital signatures, and encryption methods are supported with the summary functions should be used [12]. IoT should be preferred in banking sector, financial institutions, online services, electronic voting and critical computer networks. Using block chain-based approach in security and privacy field studies has been promising for the future of strong encryption [13].

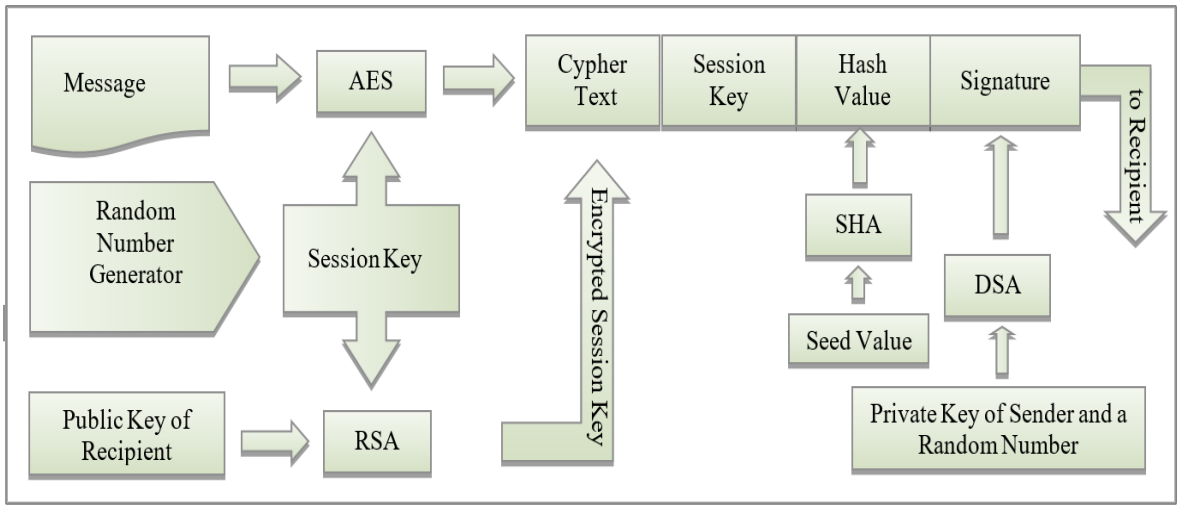


FIGURE 1. New Generation Encryption Architecture

Figure-1 shows the integrity of the data that uses encryption techniques available, providing its security and privacy structure. Encryption algorithms provide privacy and security of information against eavesdropping. A symmetric-key algorithm, like AES is used for encryption that changes the plaintext message (or transaction) into a cipher text, using a session key either generated by a random number generator or supplied by trusted key infrastructure. The session key used for encryption must be conveyed to the recipient through a secure channel. This can be done by encrypting the key with a public-key cryptography algorithm like RSA. In RSA, the public key of the recipient is used for encryption, and the recipient uses his or her private key to recover the original session key. The encrypted session key is appended to the cipher text. The appended cipher text and session key are presented to a hashing algorithm like the SHA to obtain hash value, also called a message digest (MD). Hash value is used to ensure that the cipher text + session key block is not modified or replaced by any "hacker." The sender signs the entire block by providing his or her signature that is verified by the receiver to ensure sender's identity. Signature algorithms, like DSA, help in ensuring non-repudiation in case there is a denial of sending or receiving the message in question. These four types of algorithms when judicially employed with networking protocols, can provide the most robust scheme of information exchange over a non-secure network like the internet. Once a block of information is exchanged between two participants and is further chained to subsequent blocks, it can form a secure database of information [14].

In Block cipher algorithms data is divided into blocks of the same size (New Reno Modification to data). Blocks are attached to the previous blocks with their hash (Digest) value. In this structure from the previous hash data general summary value (hash) is formed. Blocks have the transactions and the previous block address. In an unlikely occurrence of a change in one of the blocks will not permit the data verification since it will not match with the next block data key [14]. Processes are not centralized. The transaction history is added to the block chain by the approval of more than one node. Thus security validation takes place. It gives the opportunity to everybody to approve and address in a network environment which a data in the digital environment can be shared without a central authority.

11 July 2025 11:02:33

CONCLUSION

IoT technologies must be secure not only because of their efficient and flexible use, but also because of their usage in critical applications. A strong encryption algorithm makes sure that no data changes will be encountered as a result of malicious attacks or no data will be decrypted. Confidentiality of the data transferred between the sender and receiver should be secured; also correspondence and encrypted backup must be performed [15]. The new generation of encryption; the blockchain architecture, which can be done quickly and with minimum resources, is recommended. It is resistant to the attacks against changing the message [16]. It is also very efficient in terms of digital architecture, which has intense information flow of encryption and requires decryption to be done in a short time. In blockchain systems blocks grow rapidly due to saving the previous transaction records. Hereby, some performance issues can raise. Blockchain approach is suitable for IoT security and privacy [17]. AES, DES encryption is very powerful.

As a result, it is possible to say that in the IoT devices block cipher-based cyber security system is more secure than other encryption solutions. The new generation of block switching is recommended for having no limitations and rapid synchronization.

REFERENCES

[1] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," *2012 International Conference on Computer Science and Electronics Engineering,* 23 04 2012.

[2] A.-R. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) ,* 2015 07 2015.

[3] B. A. Forouzan, Data Communications and Networking, 4th edition ed., 2017.

[4] E. S. Onder Sahinaslan, "Safety in e-Transformation Applications," in *Proceedings of the International Congress on Business and Marketing'18*, Istanbul, 2018.

[5] K. Panetta, "Gartner Top 10 Strategic Technology Trends," Gartner is a registered, Florida, 2017.

[6] S. A. E. A. Canan Cimen, Cryptography in Mathematics of Passwords, Ankara: ODTU, 2009.

[7] K. L. In Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons,* no. 58, pp. 431-440, 2015.

[8] C. W. M. W. Ahmad-Reza Sadeghi, "Security and privacy challenges in industrial Internet of Things," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC),* 2015.

[9] O. Sahinaslan, "*Public E-Transformation Safety and Compliance",* Digital Transformation in Public, 1 ed., M. O. K. Gonca Telli Yamamoto, Ed., Istanbul: Kriter Publications, 2018, pp. 89-106.

[10] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)," *Computer and Communications Security Reviews,* 01 01 1996.

[11] A. K. D. Ü. Alp Öztarhan, "Nicem Hesaplama (Quantum Computation) ve Bilgi Güvenliğinin Yeni Rotaları," in *Ağ ve Bilgi Güvenliği Sempozyumu*, Istanbul, 2005.

[12] S. M. B. A. K. Akhil Kaushik, "Keyless User Defined Optimal Security Encryption," *International Journal of Computer and Electrical Engineering,* no. 2, p. 4, 2012.

[13] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain," *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* pp. 1-3, 2017.

[14] D. A. F. D. F. H. By Javaid Iqbal Zahid, "Blockchain: A Technical Overview," *IEEE Internet Policy Newsletter,* pp. 1-3, 2018.

[15] E. S. Onder Sahinaslan, "Cyber Security in Institutional E-Correspondence," in *6th International Informational Security & Cryptology Conference*, Ankara, 2013.

[16] S. C. S. K. Seyoung Huh, "Managing IoT devices using blockchain platform," *19th International Conference on Advanced Communication Technology (ICACT),* vol. IEEE, pp. 464-467, 2017.

[17] H. Li, R. Lu, L. Zhou, B. Yang and X. Shen, "An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid," *IEEE Systems Journal,* vol. 8, no. 2, pp. 655 - 663, 2014.

11 July 2025 11:02:33