How to cite this article:

Mohamed, N. N., Mohd Yussoff, Y., Saleh, M.A., & Hashim, H. (2020). Hybrid cryptographic approach for Internet of things applications: A review. *Journal of Information and Communication Technology, 19*(3), 279-319. https://doi.org/10.32890/jict2020.19.3.1

HYBRID CRYPTOGRAPHIC APPROACH FOR INTERNET OF THINGS APPLICATIONS: A REVIEW

[1]Nur Nabila Mohamed, [2]Yusnani Mohd Yussoff,
[2]Mohammed Ahmed Saleh & [2]Habibah Hashim
[1]Faculty of Engineering & Built Environment, Mahsa University, Malaysia
[2]Faculty of Electrical Engineering, Universiti Teknologi MARA, Malaysia

nurnabila.m@mahsa.edu.my; mohamedswm@yahoo.com;
yusna233, habib350@salam.uitm.edu.my

ABSTRACT

Cryptography is described as the study of encrypting or secret writing of data using logical and mathematical principles to protect information. This technique has grown in importance in computing technologies for banking services, medical systems, transportation and other Internet of Things (IoT)-based applications which have been subjected to increasing security concerns. In cryptography, each scheme is built with its own respective strength, but the implementation of single cryptographic scheme into the system has some disadvantages. For instance, symmetric encryption method provides a cost-effective technique of securing data without compromising security. However, sharing the secret key is a vital problem. On the other hand the asymmetric scheme solves the secret key distribution issue; yet the standalone technique is slow and consumes more computer resources compared to the symmetric encryption. In contrast, hashing function generates a unique and fixed-length signature for a message to provide data integrity but the method is only a one-way function which is infeasible to invert. As an alternative to solve the security weakness

Received: 20/8/2018 **Revised:** 18/6/2019 **Accepted:** 23/6/2019 **Published:** 11/6/2020

of every single scheme, integration of several cryptographic schemes which are also called the hybridization technique is being proposed offering the efficiency of securing data and solving the issue of key distribution. Herein, a review study of articles related to hybrid cryptographic approach from 2013 to 2018 is presented. Current IoT domains that implemented hybrid approaches were identified and the review was conducted according to the category of the domain. The significant findings from this literature review included the exploration of various IoT domains that implemented hybrid cryptographic techniques for improving performance in related works. From the findings, it can be concluded that the hybrid cryptographic approach has been implemented in many IoT cloud computing services. In addition, AES and ECC have been found to be the most popular methods used in the hybrid approach due to its computing speed and security resistance among other schemes.

Keywords: Cryptography, Internet of things, encryption, public key cryptography, security.

INTRODUCTION

The Internet of Things (IoT) is about connecting the unconnected. It refers to the rapidly growing internet-connected sensing devices and technologies achieving the overall perception of information, reliable transmission and intelligent processing. IoT is the combination of a variety of information sensing devices, such as radio frequency identification (RFlD), wireless sensor network (WSN), cloud computing, global positioning systems and the Internet to form a huge network and to facilitate identification and management of data, which ultimately provides the full range of services to people everywhere based on the integration of applications. The rapid development of this technology is expanding from logistics to smart neighborhood, intelligent transportation, smart banking system, and other domains. However, security issues in the entire system including devices management and deployment need to be addressed to ensure reliable and efficient services. It has been found that Man In The Middle, replay attack, spoofing and impersonation attacks are several critical threats in IoT components mainly wireless sensor network, radio frequency identification devices (RFID), cloud computing and also Machine to Machine (M2M) technology as reported by Adat and Gupta (2017). These security issues are also detected in IoT applications mostly in e-commerce, medical/ healthcare, biometric, multimedia data sharing and data transmission systems. In the attack, the malicious user may insert valid authentication tokens into a

tampered machine, booting device with a fraudulent software tool and so on. Besides, the attacker can eavesdrop on other users or data of devices that is sent over the network, masquerade as the original communicating device and reveal private data to an unauthorized third party(s). The rise of the aforesaid security and privacy problems needs further attention, thus, targeted solutions to each aspect of these issues should be provided.

Since potential attacks in IoT infrastructure could lead to loss of control of the application(s), denial of service, loss of user privacy and many other security problems, researchers believe that cryptographic approach is one of the fundamental countermeasures for securing IoT applications and its components. In practice, few cryptographic algorithms are generally combined together to strengthen security. Combining the features of several algorithms for the sake of better efficiency and performance, and for combating problems of existing algorithms is called hybrid cryptography. It is a notable technique in providing solutions to security problems in IoT to achieve several security requirements such as data confidentiality, integrity, authentication and non-repudiation properties. A number of different hybrid techniques and algorithms have been reviewed in this study, which can be used for providing security in IoT services. The remaining part of the paper is organized as follows. The next section describes the research methodology, and then hybrid approaches which are categorized into several IoT domains. This is followed by an analysis and discussion and the last section concludes the work.

RESEARCH METHODOLOGY

The aim of this study is to provide a review of the selection of hybrid cryptographic approach in IoT domains based on the current literature. There are two research questions in this study: 1. What are the domains of IoT where hybrid cryptographic approaches are used and which type of algorithms are proposed in the domain? 2. What are the most frequently used algorithms for symmetric and asymmetric schemes in the approach? Based on these research questions, two objectives have been formulated. The first objective of this study is to explore the IoT domains that implement hybrid cryptographic approaches and the types of cryptographic schemes used in each domain. The second objective is to identify the most frequently used cryptographic methods in the approach for symmetric and asymmetric schemes. To achieve the first objective of this study, the articles on hybrid security approaches related to IoT components and its application technology from 2013 to 2018 were reviewed. Keywords of "hybrid security approach and Internet of Things" were searched in the electronic databases in the Web of Science, Scopus and

IEEE Xplore search engines. After locating approximately 126 papers related to the approaches, a deep topic filtering was conducted. Consequently, 89 publication articles that satisfied the requirements were selected. In this paper, current IoT domains that implemented hybrid approaches were identified and the review was conducted according to the category of the domain. Based on the review, several IoT fields that implemented the hybrid technique were identified and categorized into several domains, which were WSN, RFID, cloud computing and data storage, multimedia data, data transmission, information security, smart healthcare and medical system, smart grid, fog computing, biometric and smart banking. The second objective was achieved by classifying the cryptographic methods which are listed in tables according to each domain in the next section. After the classification, the most popular symmetric and asymmetric schemes were identified and the results discussed in the Discussion section.

REVIEW OF HYBRID CRYPTOGRAPHIC APPROACHES

Security is an important component for the property of systems to ensure that resources of value cannot be altered, copied or made available to malicious users. Every system design requires a different set of security properties such as data confidentiality, integrity, authentication and availability that depends on the type and value of the assets to defend against malicious attack. To achieve these security properties, various security mechanisms have been developed which generally utilize cryptographic schemes such as symmetric and asymmetric encryption, hash function, entity authentication, key agreement and others. Common cryptographic techniques can be classified into three groups which are symmetric encryption, asymmetric encryption and cryptographic hash function. According to Bellare, Desai, Jokipii and Rogaway (1997), symmetric encryption algorithm utilizes a single secret key to encrypt and decrypt the information. This algorithm is quite efficient in terms of speed and computing power because it implements only one key. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two well-known symmetric algorithms, yet AES is more powerful than DES in terms of security strength. Other examples of symmetric algorithms are 3DES, RC2, RC4, RC6 and Blowfish schemes. Referring to related work by Ma and Jin (2018), although symmetric encryption is extremely fast in terms of computation, it has weakness in key distribution. In order to implement symmetric encryption on public communication, the secret key must be shared securely and secretly with an authorized communicating party which is the main difficulty in this approach (Zakir & Sarker, 2005).

In contrast, the asymmetric key, also known as public key cryptography requires

the use of two different keys to encrypt and decrypt data; a private key that is only known and must remain confidential to its respective owner for decryption, and a public key that is known to other entities on the public network. In this system, the key which is revealed to the public is used to encrypt data, while the other key which is kept secret, is used to decrypt the data. Common asymmetric key algorithms are Rivest, Shamir and Adleman (RSA), Diffie Hellman Key Exchange (DHKE) key agreement protocol, El Gamal, Elliptic Curve Cryptography (ECC). These algorithms are used to ensure the security properties of data confidentiality, authenticity and non-repudiability. The disadvantage of the asymmetric scheme is the speed; it is much slower than symmetric encryption because the computations are comparatively complex, which means that the message takes more time to be encrypted and decrypted as reported by Li, Chen, Qin, and Wan (2010). Meanwhile, few asymmetric schemes such as DHKE and El Gamal can also be used to provide a secure method for key negotiation in public channels. Despite this, it has the risk of being intercepted by Man-In-The-Middle (MITM) during the key exchange between those involved in the process.

According to Gallagher (2012), another method known as cryptographic hash function is used for verification purposes such as for signatures and certification processes. The hash value is a cryptographic checksum that both communicating parties must compute for message verification. The sender uses a hash function to perform the checksum for the message, which is sent together with the message to the receiver. The receiving side must compute the hash value on the received message which must turn out to be the same. If the message has been changed during transmission by other malicious users, the hash values will be different and the packet is rejected. The most widely used hash functions nowadays are: Secure Hash Algorithm (SHA1), SHA2, SHA3 and Message Digest 5 (MD5). However, the drawback of the method is that the hash function always produces the same value for specific input. Once the attacker obtains the value, he/she can assume whatever security identity associated with the hash as reported by Kessler (1998).

Above all, the implementation of single cryptographic algorithm has several weaknesses. Key management is a significant problem in the symmetric encryption technique while asymmetric encryption provides efficient key maintenance but has relatively low performance in terms of time. In addition, the hashing technique should be integrated with the encryption method to enhance security and ensure data integrity. Thus, the hybrid cryptographic approach which combines symmetric, asymmetric and hash function can contribute to optimum security with minimized key maintenance, and also ensures that the original text is not altered in the communication medium (Dubai, Mahesh & Ghosh, 2011). In practice, few cryptographic algorithms are generally combined together to strengthen

security. Combining the features of a few algorithms for the sake of better efficiency and performance, and for combating the constraints of independent algorithms is known as hybrid cryptography. Hybridization is a notable technique providing solutions to some major problems such as computing speed, performance or any other means to achieve optimum security level of a system(s). Review studies of existing hybrid approaches to secure the M2M system were conducted to explore the findings of different cryptographic schemes used in the different domains. This will help researchers in identifying the most suitable or feasible cryptographic scheme for their specific studies or applications.

Hybrid Security Approach in WSN Related-IoT

WSNs are considered as one of the core technologies in implementing IoT architectures. WSNs are vulnerable to security attacks due to the broadcast nature of the transmission medium. Since WSN has limited energy and processing power for nodes, it makes it quite difficult to implement traditional security algorithms for these networks. To restrain these issues, various security algorithms have been proposed in order to achieve security requirements, i.e. confidentiality, authentication and integrity. Six papers were found to propose the hybrid approach to secure the WSN related-IoT applications. Rizk and Alkady (2015) presented a hybrid security approach by applying two different techniques to secure two splitting plaintexts. The first part of the data was protected using a combination of symmetric and asymmetric AES-ECC, while the other part was secured using XOR-DUAL RSA. MD5 hash function was also implemented as integrity check.

This work evaluated several performance metrics such as ciphertext size, encryption/ decryption time, time complexity, energy and the rate of dropped packets. Another work by Moon and Ingole (2015) proposed a hybrid approach using cellular automata based security algorithms (CAWS) for key management and modern encryption standard version1 (MES-1) symmetric scheme for encryption/decryption data in WSN system. The method provided positive performance against intrusion attack, less power transmission, receiver collision problem, etc. Meanwhile, Kavitha and Caroline (2015) introduced the hybrid key management method (HKM) by enhancing asymmetric encryption, and ECDH for key management. This work evaluated energy consumption; however, the method used for data encryption was not mentioned. Qi, Hu, Ma and Sun (2015) constructed a lightweight hybrid strategy known as MA-CBE, by using a combination of 8-bit chaotic block encryption and Message Authentication Code (MAC) based hashing. The work evaluated compression ratio, input data size, data correlation, energy consumption and saving. The results showed that this scheme gave significant

performance in terms of security and energy-efficiency to solve the energy constraints of WSN. Yin and Liang (2014) proposed a certificateless hybrid signcryption scheme using key-encapsulation and data-encapsulation by using random oracle model. The scheme is suitable in securing WSN communication protocols for key management and secure routing. The performance metrics of computational complexity and ciphertext length were evaluated. Zhong, Shao, Cui and Xu (2018) proposed a mixed of concealed data aggregation (CDA) based on homomorphic encryption technology with a signature scheme. The combined method produced large aggregated results with the analysis of the scheme's functionality, computation overhead, energy consumption and delay. Table 1 summarizes the related works which implement the hybrid approaches in WSN related-IoT. It has been noted that most of the works evaluated energy consumption which indicates that this metric is important in WSN field. In addition, out of the six publications, five of them presented security analysis to prove that hybrid methods can strengthen the network.

Table 1

Hybrid Security Approach in WSN Related-IoT

Study	**Method**	**Performance Metrics**	**Is security analysis/proof presented?**
Rizk and Alkady (2015)	AES-ECC, XOR DUAL RSA and MD5	Ciphertext size, encryption/decryption time, time complexity, energy consumption, rate of dropped packets	Yes
Moon and Ingole (2015)	CAWS and MES-1	Adhoc on demand distance vector and Enhanced Adaptive cknowledgment	Yes
Kavitha Caroline (2015)	ECC and DHKE	Energy consumption and resilience	No
Qi et al. (2015)	8-bit chaotic block encryption and MACs based hashing	Compression ratio, input data size, data correlation, energy consumption and saving	Yes

(continued)

Study	Method	Performance Metrics	Is security analysis/proof presented?
Yin and Liang (2014)	Certificateless hybrid signcryption scheme using key-encapsulation and data-encapsulation in random oracle model.	Computational complexity and ciphertext length	Yes
Zhong et al. (2018)	Homomorphic Encryption (HE) and signature scheme.	Functionality, computation overhead, energy consumption, delay	Yes

HYBRID SECURITY APPROACH IN RFID RELATED-IOT

Other than WSN technology, the hybrid approach has been in demand in many RFID technologies. RFID is described as a key technology enabler for the IoT. However, the tags which are not protected appropriately may be easily targeted for eavesdropping, DoS attacks, traffic analysis and other vulnerabilities. Hence, the system still needs appropriate hybrid techniques bearing in mind the total cost associated with them. Sharma and Singh (2017) proposed a hybrid algorithm using PICO Ultra Lightweight cipher and 128 bit random streams as authentication input for data security.

The author evaluated the avalanche effect, plaintext sensitivity, key sensitivity, correlation, execution time, and brute force combination. Jeddi, Amini and Bayoumi (2013) combined a new symmetric block cipher called, Redundant Bit Security (RBS) with MAC algorithm to be used as redundant bits and merged them with altered original bits. Two metrics were evaluated in this study which consisted of the reported area and power figures. Another hybrid method was by Bu and Li (2018). The author proposed an implementation of STEPAUTH based on the Elliptic Curve Integrated Encryption Scheme (ECIES) and the Elliptic Curve Digital Signature Algorithm (ECDSA). It was found that the method was faster with short key yet guaranteed the same level of security as RSA which also showed a significant performance in efficient memory and computation cost. Lin, Kang and Shi (2013) and Bhave and Jajoo (2015) took advantage of both the symmetric and asymmetric schemes by hybridizing AES and ECC. The method proposed by Lin et al. (2013) can protect users' privacy and implement access controls, however, no performance evaluation was presented. Bhave and Jajoo (2015) combined the AES-ECC to secure key exchange and enhanced ciphertext security. The test results of bit error rate and signal to noise ratio were analyzed which showed the decrease in bit error rate when compared to single encryption. From Table 2, it can be

summarized that work by Sharma and Singh (2017), Lin et al. (2013) and Bhave and Jajoo (2015) combined the symmetric and asymmetric algorithms to strengthen the security of RFID systems. Besides, it can be seen that the work by Jeddi et al. (2013) and Bu and Li (2018) also integrated MAC and Digital Signature Algorithm to provide data authentication in the system.

Table 2

Hybrid Security Approach in RFID related-IoT

Study	Method	Performance Metrics	Is security analysis/ proof presented?
Sharma and Singh (2017)	PICO Ultra Lightweight cipher and 128 bit random streams as authentication input	Avalanche effect, plaintext sensitivity, key sensitivity, correlation, execution time, brute force combination	Yes
Jeddi et al. (2013)	New symmetric block cipher called RBS and MAC scheme	Reported area and power figures	No
Bu and Li (2018)	ECIES and ECDSA	Memory cost and computation cost	Yes
Lin et al. (2013)	AES and ECC	No performance evaluation	No
Bhave and Jajoo (2015)	AES and ECC	Bit error rate and signal to noise ratio	No

HYBRID SECURITY APPROACH IN CLOUD AND DATA STORAGE

Cloud becomes an ideal storage location for storing and processing IoT data but there are some problems in using the cloud and data Storage in IoT. There may be a possibility that privacy rights will not be followed by cloud service providers. To deal with this issue cryptographic techniques is proposed. The hybrid approach has been introduced in 17 publications in cloud and data storage related to IoT applications which is summarized in

Table 3. Goyal and Kinger (2013) presented the hybrid of three encryption mechanisms: Caesar, Rijndael algorithm and Vernam cipher. The key should be at least as long as the message and is truly random. The approach was not compared with other work to observe its performance.

Gajra, Khan and Rane (2014) proposed the hybridization of AES and Blowfish for data encryption. For key management and key exchange, the key was generated using ECC key generator and the key agreement was performed using Diffie-Hellman. The web page system architecture was built to test the proposed approach; however, no performance analysis was executed. Mahalle and Shahade (2014) proposed the hybrid approach by using RSA and AES algorithms for providing data security to the user in the cloud. The approach was tested on upload and download module based on cloud architecture but no performance analysis was executed. Sengupta and Chinnasamy (2015) designed a hybrid algorithm known as DESCAST to provide the security of huge data volume sent through the cloud. The size of the ciphertext using the algorithm was the same as that of individual DES or CAST. Sujithra, Padmavathi and Narayanan (2014) proposed a three-tier security approach. In the first-tier, encryption was performed using the MD5 algorithm. In the second-tier, encrypted data was re-encrypted using AES. In the third-tier, further encryption of data or key using ECC or RSA algorithm was performed respectively.

The combination of MD5+ECC+AES showed better performance in terms of Speed-Up ratio. Poornima and Rajendran (2014) suggested hierarchical attribute-set based encryption (HASBE) by expanding ciphertext-policy attribute set-based encryption (ASBE) with a hierarchical structure. The system and security model was designed but the hybrid approach was not clearly explained. In addition, no evaluation was conducted to analyze its performance. Cheon and Kim (2015) introduced hybrid encryption combining public-key encryption (PKE) and somewhat homomorphic encryption (SHE) to reduce storage requirements. By evaluating the ciphertext size and the expansion ratio, the approach provided a trade-off between the size of the transmitted ciphertexts and conversion costs. Lin, Zhang, Ma and Wang (2015) proposed more efficient and generic construction of attribute-based encryption (ABE) with verifiable outsourced decryption, a symmetric-key encryption scheme and a commitment scheme. From the results of the encryption and decryption time, ciphertext size and transform time, the proposed scheme reduced bandwidth and computation costs almost by half.

Sharma and Joshi (2017) proposed a novel hybrid cloud security method using a combination of two well- known security techniques, IBE and ABE. The revocation efficiency was improved by 40% as compared to the existing method. Kirichek, Kulik and Koucheryavy (2016) proposed

RSA-512 for public key generation and AES-128 for data protection. The method was tested on MQTT protocol to prove it was suitable for the majority of IoTs; yet the study presented no performance evaluation. Bansal and Singh (2016) presented a hybrid cryptosystem using RSA and Blowfish algorithm. The FPGA device Virtex-4 was used for implementation using Xilinx ISE 14.1. The proposed hybrid technique served both symmetric and asymmetric properties. Chauhan and Gupta (2017) proposed a novel parallel cryptographic algorithm, blending and changing from MD5 and Blowfish encryption schemes to upgrade security. From the results of encrypted file size, encryption and decryption time, it was found that hybrid symmetric and hashing method (Blowfish- MD5) generated less execution time in comparison to hybrid asymmetric and hashing (RSA-MD5). Olumide, Alsadoon, Prasad and Pham (2015) identified available solutions using encryption technology in cloud computing. A hybrid scheme using AES and fully homomorphic encryption (FHE) was proposed. The analysis indicated that the proposed AES-FHE scheme had high efficiency and security compared to AES-RSA in terms of the number of encryption, number of keys generated, key expiration, pre-encryption, key generation, save passage during transfer, user verification, process speed on large files, and security application.

Kaushik and Gandhi (2016) proposed hybrid encryption concepts using the symmetric and asymmetric method to provide a protected environment for cloud data storage. The system uses Cloud Service Provider as the third party to store data. Bhandari (2016) proposed a hybrid RSA (HE-RSA) along with AES to ensure efficiency, consistency and trustworthiness in cloud servers. From the results, the execution time when using the hybrid approach was reduced to 20%. Maitri and Verma (2016) introduced hybrid security using symmetric algorithm and steganography methods. AES, blowfish, RC6 and BRA symmetric algorithms were used to provide block-wise security. LSB steganography technique was introduced for key information security. Data integrity was accomplished using SHA1 hash function. The proposed technique reduced 20% execution time and produced smaller text size as compared to the single scheme. Kanna and Vasudevan (2016) proposed a novel identity-based hybrid encryption using RSA and ECC. In the first phase, user data was encrypted with receiver identity. In the second phase, the identity and keyword were encrypted using PRE. The hybrid approach was more efficient in terms of execution time and throughput. Above all, from Table 3, it can be seen that only a few number of studies presented the security analysis and performance evaluation which may be because the work was only intended to demonstrate the system model and web page development.

Table 3

Hybrid Security Approach in Cloud and Data Storage

Study	Method	Performance Metrics	Is security analysis/proof presented?
Goyal and Kinger (2013)	Caesar, Rijndael algorithm and Vernam cipher	No performance evaluation	No
Gajra et al. (2014)	AES, Blowfish, ECC and DHKE	No performance evaluation	No
Mahalle and Shahade (2014)	RSA and AES	No performance evaluation	No
Sengupta and Chinnasamy (2015)	DESCAST	Ciphertext size	No
Sujithra et al. (2014)	MD5-AES-ECC and MD5- AES-RSA	Mean processing time, encryption and decryption time, speed up ratio	No
Poornima and Rajendran (2014)	HASBE and ciphertext policy ASBE	No performance evaluation	No
Cheon and Kim (2015)	PKE and SHE	Ciphertext size, expansion ratio	No
Lin et al. (2015)	ABE with verifiable outsourced decryption, a symmetric-key encryption scheme and a commitment scheme	Encryption time, ciphertext size, transform time, decryption time	Yes
Sharma and Joshi (2017)	IBE and ABE	Time cost for key update, encryption time	No
Kirichek et al. (2016)	RSA-512 and AES-128	No performance evaluation.	No
Bansal and Singh (2016)	RSA and Blowfish	No performance evaluation	No
Chauhan and Gupta (2017)	Blowfish-MD5 and RSA-MD5	Encrypted file size, encryption and decryption time	No

(continued)

Study	Method	Performance Metrics	Is security analysis/proof presented?
Olumide et al. (2015)	AES and Fully Homomorphic Encryption FHE and AES-RSA	Number of encryption, number of keys generated, key expiration, pre encryption, key generation, save passage during transfer, user verification, process speed on large files	Yes
Kaushik and Gandhi (2016)	Symmetric and asymmetric methods	No performance evaluation.	No
Bhandari (2016)	AES, homomorphic encryption and RSA	Total execution time	Yes
Maitri and Verma (2016)	AES, blowfish, RC6 and BRA, LSB steganography technique and SHA1	Encryption and decryption time	No
Kanna and Vasudevan (2016)	RSA, ECC and PRE	Encryption and decryption time, throughput, total execution time	No

HYBRID SECURITY APPROACH IN SMART HEALTHCARE/ MEDICAL SYSTEM

The IoT in healthcare and medical system is the key player in providing better medical facilities to patients and in facilitating doctors and hospitals as well. The IoT devices monitor patients' health, and upload collected data to the cloud for storage and sharing. In response to the increasing security challenges in the system, researchers have proposed many schemes for data confidentiality and privacy. A total of 10 papers have introduced the hybrid method in smart healthcare and medical system which is related to IoT applications. Gonçalves, Leonova, Puttini and Nascimento (2015) presented the hybrid public-key infrastructures using HMAC, AES and RSA to store electronic medical records on the cloud, while preserving privacy. The approach combined hashing, symmetric and asymmetric algorithm to achieve complete security property, but no performance metric was presented. Al-Haj, Abandah and Hussein (2015) introduced strong cryptographic functions with internally generated symmetric keys and hash codes to provide confidentiality, authenticity and integrity of medical images exchanged in telemedicine apps.

The algorithms presented confidentiality, authenticity and integrity for header data, as well as for pixel data of DICOM images. A year later, the same authors Al-Haj et al. (2016) proposed a combination of hash function and watermarking techniques to authenticate the owner of x-ray image and protect its integrity.The enhanced technique was compared with the original image to evaluate peak signal to noise ratio (PSNR). Smithamol and Rajeswari (2017) proposed privacy- aware security framework, Group CP-ABE consisting of two phases of encryption. In phase 1, the EMR database was encrypted using AES-256 bit key, and in phase 2 the keys used for symmetric encryption were encrypted using CP-ABE. The experimental analysis based on several metrics such as key generation time, encryption time, decryption time, re-encryption time and computation overhead indicated the efficiency of the approach to reduce overall computation overhead. Dahiya and Bohra (2017) proposed a robust and complex encryption model, defined as the parallel partial model (PPM) which was collaborated with the improved Advanced Encryption Standard (iAES) and modified Elliptic Curve Cryptography (mECC).

The result showed that it was more efficient than the existing model in terms of bit difference, overall time and average time. Bouchti, El Bahsani and Nahhal (2016) proposed a hybrid architecture based on Cryptography as a Service (CaaS) including private cloud OpenStack platform. Hybrid homomorphic encryption and RSA were implemented in the proposed architecture. The implementation offered a fast point multiplication, while featuring small code and memory requirements. Bala, Maity and Jena (2017) proposed a secure key management and authentication protocol, making use of hybrid cryptography involving both symmetric and certificate-less public key cryptographic algorithms. The applied symmetric algorithms, AES-CCM provided assurance of both data authenticity and confidentiality by the evaluation of computation cost and benchmark on the average time. Zhai, Ait Si Ali, Amira and Bensaali (2017) presented a set of security solutions implementing AES and electrocardiogram (ECG) identification system. The proposed AES and ECG identification outperformed existing field programmable gate array (FPGA)-based systems in processing time, hardware resources and power consumption. Alanazi, Zaidan, Kiah and Al-Bakri (2015) proposed a technique that integrated AES and NTRU algorithms to maintain the secrecy of transmitted Electronic Medical Records.

Integrating two powerful algorithms created a powerful algorithm that ultimately provided excellent security in transmitting EMRs. Belkaid, Mourad, Mehdi and Soltane (2015) presented a new encryption system combining AES-RSA for secure medical image transmission. The AES was used for data confidentiality while the RSA was used for authentication, and integrity was assured by the correlation between adjacent pixels image. Studies by

Gonçalves et al. (2015), Smithamol and Rajeswari (2017), Dahiya and Bohra (2017), Bala et al. (2017), Zhai et al. (2017), Alanazi et al. (2015) and Belkaid et al. (2015) showed that the AES scheme gave good property in decreasing the correlation and outperformed algorithms studied in the literature. A summary of the related works is presented in Table 4.

Table 4

Hybrid Security Approach in Smart Healthcare and Medical System

Study	Method	Performance Metrics	Is security analysis/proof presented?
Gonçalves et al. (2015)	HMAC, AES and RSA	No performance evaluation	Yes
Al-Haj et al. (2016)	Hash function and Watermarking technique	Peak signal to noise ratio (PSNR)	Yes
Smithamol and Rajeswari (2017)	AES-256 and CP- ABE	Key generation time, encryption time, decryption time, re-encryption time, computation overhead	Yes
Dahiya and Bohra (2017)	iAES and mECC	Encryption time and average encryption time	No
Bouchti et al. (2016)	Homomorphic encryption and RSA	No performance evaluation	No
Al-Haj et al. (2015)	Symmetric keys and Hash codes	Correlation factor, PSNR value, entropy value, encryption and decryption time	Yes
Bala et al. (2017)	AES, Certificateless Cryptographic Method CCM and SHA1	Computation cost, benchmark on average time	Yes
Zhai et al. (2017)	AES and ECG identification system	ECG amplitude, processing time and hardware utilization estimate of each block, hardware resource usage, power consumption, processing speed, throughput	No

(continued)

Study	Method	Performance Metrics	Is security analysis/ proof presented?
Alanazi et al. (2015)	AES and NTRU	No performance evaluation	No
Belkaid et al. (2015)	AES-RSA	Histogram analysis, correlation, key sensitivity, correlation coefficient, execution time	Yes

HYRID SECURITY APPROACH IN MULTIMEDIA DATA IN IOT

The widespread use of multimedia data applications in IoT service is emerging as a serious threat in terms of the privacy, well-being, and safety of organizations and individuals. In multimedia applications, the confidentiality and security of the data captured from multimedia device are very important. A total of 15 articles in this review proposed the use of the hybrid technique in multimedia data in IoT services and this is summarized in Table 5. Quist-aphetsi, Nana and Pascu (2013) proposed a hybrid method based on asymmetric encryption algorithm and visual cryptographic algorithm. The algorithm was implemented using MATLAB on specific image size. The effectiveness and robustness of the ciphering process depended on the length of the shared secret key and the computer resources available (processing power and speed). Sridhar Iyer, Sedamkar and Gupta (2016) proposed hybrid cryptographic technique comprising of a mix of symmetric and asymmetric ciphers, AES and ECC. The proposed approach yielded better outcomes in terms of visual test, execution time, mean gray level and PSNR value. Zhao, Ran and Chi (2015) proposed an improved method using RSA based on existing OACS and the new system conformed to the basic agreement of public key cryptosystem. By evaluating the performance of visual test, mean square error (MSE), SNR, PSNR and correlation coefficient, the hybrid method showed the validity of the improved cryptosystem and high robustness against attacks.

Dawahdeh, Yaakob and Razif (2017) proposed a new image encryption technique combining ECC with Hill Cipher (ECCHC) to convert Hill cipher from a symmetric to an asymmetric one. Self-invertible key matrix is used to generate the secret key. The proposed approach has a simple structure and faster computations. Bisht, Thomas and Thanikaiselvan (2017) proposed a hybrid technique including two phases of work simultaneously. In Phase-1, it took advantage of the benefits of both symmetric and asymmetric

techniques using AES and RSA. In Phase-2, encrypted data obtained from the latter algorithms were given to the Difference Expansion (RDH) system. The combination of AES–RSA with RDH to obtain a double layer of security provided a high operation speed and security performance.

Iyer, Sedamkar and Gupta (2016) proposed the implementation of a system capable of encrypting/decrypting multimedia data (text, images, videos) using the hybrid model of AES and ECC. It was found that even if an attacker gets access to the keys; he/she will not be able to decipher it in a relatively finite amount of man-years. However, this study did not provide a performance evaluation. Chaturvedi and Jain (2016) proposed an improved cryptography system based on RSA and RC6. Four different keys were needed for the decryption process along with the extra shifting of pixels by XOR. The less variety in entropy was accomplished from the methodology which showed the efficiency of the approach. Sharma and Chopra (2017) performed the encryption and decryption using AES whereas ECDH was used for the session set up between client and server. Diffie-Hellman was also implemented to establish shared secrets after the key agreement. The result indicated that the proposed approach gave better performance in terms of avalanche and correlation. Manjula and Shivakumar (2016) hybridized AES and ECC for data encryption. The double encrypted data was then compressed with Lempel Ziv welch technique to reduce the residing capacity of data. Implementation of the symmetric and asymmetric algorithm made visual and statistical attacks more resistive.

Kester, Nana, Pascu and Gire (2013) proposed the modified of DHKE algorithm to exchange key, and then hash using MD5 algorithm. The results of the visual test and histogram analysis indicated that the implementation in hardware and software systems produced a delay in streaming video images. Saini and Verma (2013) proposed a new version of the AES algorithm to encrypt the image, which was hidden into a cover image using the steganography concept. The hybrid approach provided greater performance in terms of visual test, histogram analysis, correlation coefficient (CC), PSNR, and MSE when compared to single AES. Ramesh and Jain (2015) introduced a two-stage image encryption using two Pseudo-Random Number Generators. In the first stage, altered version of Sophie Germain Prime Generator was used to create generated pseudo-random numbers. In the second stage, Lehmer RNG was used to generate random numbers. The visual and statistical tests showed the high security levels of the hybrid encryption algorithm.

Gupta, Alra and Hasti (2016) developed a new algorithm to hide data inside images combining both steganography and cryptography. Textual data was encrypted using AES, and then stored in color images using hash-based algorithm. The proposed scheme was applied to different image types and it did not corrupt the image quality in any form. According to the approach

proposed by Saleh, Aly and Omara (2016), firstly the secret data was encrypted by using the AES-MPK then the encrypted data was hidden in gray image by using PVD-MPK and MSLDIP-MPK steganography methods. The hybrid approach provided two levels of security, high embedding capacity and high quality of stegano images. Kotel et al. (2016) proposed hybrid video cryptosystem combining two techniques: the chaos and AES in CTR mode. From the analysis of frequency, power consumption, block RAM, throughput and throughput per slice, the combined approach demonstrated that the cryptosystem is a highly efficient and robust system for video encryption. From Table 5, it can be concluded that visual test and histogram analysis are important metrics to evaluate multimedia performance.

Table 5

Hybrid Security Approach in Multimedia Data Related-IoT

Study	**Method**	**Performance Metrics**	**Is security analysis/proof presented?**
Quist-aphetsi et al. (2013)	Asymmetric encryption and visual cryptographic algorithm	Permutation, ciphering image	No
Sridhar C Iyer et al. (2016)	AES and ECC	Visual test, execution time, mean gray level, PSNR value	Yes
Zhao et al. (2015)	RSA and OACS	Visual test, MSE, SNR, PSNR, correlation coefficient	Yes
Dawahdeh et al. (2017)	ECCHC	Visual test, histogram analysis, PSNR, UACI, encryption and decryption time	Yes
Bisht et al. (2017)	AES and RSA	Visual analysis, PSNR, correlation, encryption time, NCPR, UACI, histogram analysis	Yes

(continued)

Study	Method	Performance Metrics	Is security analysis/proof presented?
Iyer et al. (2016)	AES and ECC	No performance evaluation.	Yes
Chaturvedi and Jain (2016)	RSA and RC6	Visual test, histogram analysis, correlation, information entropy	Yes
Sharma and Chopra (2017)	AES, ECC and DHKE	Ciphertext size, encryption and decryption time, avalanche effect, correlation	Yes
Manjula and Shivakumar (2016)	AES and ECC	PSNR	No
Kester et al. (2013)	Modified DHKE algorithm and MD5	Visual test, histogram analysis	No
Saini and Verma (2013)	New version of AES algorithm and steganography technique	Visual test, histogram analysis, correlation coefficient (CC), PSNR, MSE	Yes
Ramesh and Jain (2015)	Sophie Germain Prime Generator and Lehmer RNG	Visual test, histogram analysis, entropy value, NPCR, UACI, CC	Yes
Shreya and Akshay (2016)	AES and steganography	Visual test, MSE	No
Saleh et al. (2016)	AES-MPK and PVD-MPK	Visual test, histogram analysis, hiding capacity, PSNR, encrypt time, hiding time, extract time, decrypt time	No
Kotel et al. (2016)	Chaos and AES-CTR mode	Frequency, power consumption, block RAM, throughput, throughput per slice	Yes

HYBRID SECURITY APPROACH IN DATA TRANSMISSION RELATED-IOT

The IoT devices should provide robust communication channel capacity for securing data transfer of diverse types of data in order to prevent data transmission against cyberattacks. A total of 14 studies showed that the hybrid approach was also presented in data transmission related-IoT applications. Hong, Qiu, Zeng, Wang and Sandrine (2017) proposed a new concept of fusion encryption for monitoring equipment: the communication data is encrypted by the hybrid encryption algorithm based on DES and RC4 fusion encryption algorithm, and the core encryption merges two symmetric encryption methods to form a new encryption algorithm. This study, however, presented no performance evaluation. Xin (2015) proposed a mixed encryption using AES and ECC. MD5 was integrated with ECC and AES to form a hybrid approach. From the results of key exchange time, number of time, key length, time of signature, number of signatures and verification time, it showed that the improved ECDH method was three times faster than the original ECDH. Hong and Xuefeng (2013) presented a security framework using handshake agreement, SM2 resolving security problems between client and receptor in the information transmission process.

The algorithm was carried out using a wide range of IoT based on elliptical graph of ECC. No performance evaluation was presented in this article. Fei, Li, Yang and Li (2016) proposed a secure and efficient file protecting the system (SEFPS) based on advanced SHA3 and parallel AES to produce high performance via Graphics Processing Unit parallelism and Central Processing Unit parallelism. A total of six algorithms were designed based on SHA3 and AES method to observe the most feasible algorithm. The performance metrics evaluated in this article were total protecting speed, encryption speed, hash speed, protecting speedup, encryption speedup, parallel efficiency, total unprotecting speed, decryption speed, and decryption speedup. Harba (2017) proposed a method using hybrid techniques: symmetric AES to encrypt files, asymmetric RSA to encrypt AES password and HMAC to encrypt symmetric password/data. The results of the ciphertext size and encryption time indicated that the overall encryption yielded low computational requirements and provided high security. Amandeep (2016) presented a new hybrid scheme based on Fibonacci series, XOR cipher, PN sequence, RSA, Hill cipher, one bit LSB, two bit LSB and three bit LSB. The application of five different techniques to different segments of the same message along with the symmetric key and asymmetric key and three types of LSB provided confidentiality and authentication of data.

Qiu, Ma and Chen (2017) applied hybrid technique which involved certificateless cryptography and AES to achieve the authentication and

anonymity properties. The approach was tested on windows and android platforms to evaluate computation cost and time consumption. The security analysis with Burrows–Abadi–Needham (BAN) logic and the Automated Validation of Internet Security Protocols and Applications (AVISPA) showed that the proposed scheme was well designed and could withstand MITM attacks, replay attacks, DoS attacks, impersonation attacks and compromised attacks. Altigani and Barry (2013) proposed a new approach combining AES and steganography Word Shift Coding Protocol. AES was used to equip "secret" data with initial confidentiality layer; the encrypted data were represented in binary, and hidden in the textual carrier. Experimental results showed significant delays which was attributed to many reasons such as the cost of checking all the cover characters. D'souza and Panchal (2017) proposed AES with a hybrid approach of Dynamic Key Generation and Dynamic S-box Generation. More complexity in data was added to increase Confusion and Diffusion in cipher text using Dynamic Key Generation. The proposed approach protected the message from Brute-force, Differential Attack, Algebraic and Linear Attack.

Zhang, Zheng, Chen, Li and Li (2016) presented a generic attribute-based data sharing system based on a hybrid mechanism of CP-ABE and a symmetric encryption scheme. From the results of the computation cost, system setup time, key generation time, encryption and decryption time, it was found that the proposed CP- ABE scheme was proven selective-secure in the random oracle model under the decision n-BDHE assumption. Purevjav, Kim and Lee (2016) designed a new protocol using symmetric cipher Ping Pong-128 and RSA with hash function MD5. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. You, Shi, Chen, Qi and Qing (2017) implemented DH key exchange on the matrix platform, and an improved key negotiation algorithm was proposed to obtain the negotiation key before exchanging the intermediate value. The necessary and sufficient conditions for the fourth order reversible matrix on the finite field GF(28) were obtained by studying the reversible matrix. Singh et al. (2015) proposed a hybrid approach consisting of four phases, based on symmetric encipherment.

The technique reduced data size by 50% and strengthened security by relating the plaintext character with its position in text for generating the corresponding ciphertext. Abdelgader, Wu, Simik and Abdelmutalab (2015) presented a security system based on the use of AES, IDEA and RSA. The proposed system also implemented public key cryptosystem and one-way hash function to provide integrity, authentication and efficient key distribution. The proposed hybrid approach solved the key distribution problem by using RSA public key cryptography systems. The following Table 6 is a summary of related works in the data transmission field. Based on

the table, several studies such as by Xin (2015), Harba (2017), Purevjav et al. (2016) and Abdelgader et al. (2015) combined three types of cryptographic schemes which consisted of symmetric, asymmetric and message digest to strengthen security. According to the table, it is noted that encryption and decryption time are significant metrics in evaluating performance for IoT data transmission. However, some of the studies did not provide performance evaluation and security analysis.

Table 6

Hybrid Security Approach in Data Transmission Related-IoT

Study	Method	Performance Metrics	Is security analysis/proof presented?
Hong et al. (2017)	DES and RC4	No evaluation	No
Xin (2015)	MD5, AES and ECDH	Key exchange time, number of time, key length, time of signature, number of signature, verification time	No
Hong and Xuefeng (2013)	Handshake agreement (SM2) and ECC	No performance evaluation	No
Fei et al. (2016)	SHA3 and parallel AES	Total protecting speed, encryption speed, hash speed, protecting speedup, encryption speedup, parallel efficiency, total unprotecting speed, decryption speed, decryption speedup	Yes
Harba (2017)	AES, RSA and HMAC	Ciphertext size, encryption time	No
Amandeep (2016)	Fibonacci series, XOR cipher, PN sequence, RSA, Hill cipher, one bit LSB, two bit LSB and three bit LSB	MSE, root MSE, PSNR	No
Qiu et al. (2017)	Certificateless cryptography and AES	Computation cost, time consumption on windows and android	Yes

(continued)

Study	Method	Performance Metrics	Is security analysis/proof presented?
Altigani and Barry (2013)	AES and steganography Word Shift Coding	Encryption time and extraction time	No
D'souza and Panchal (2017)	AES and Dynamic Key Generation and Dynamic S-box Generation	Encryption and decryption test	No
Zhang et al. (2016)	Ciphertext-policy attribute-based encryption (CP-ABE) and a symmetric encryption scheme	Computation cost, system setup time, key generation time, encryption and decryption time	Yes
Purevjav et al. (2016)	Symmetric cipher Ping Pong-128, RSA and hash function MD5	Encryption and decryption test	No
You et al. (2017)	DH key exchange and an improved key negotiation algorithm	No performance evaluation	Yes
Singh et al. (2015)	Symmetric encipherment and middle value algorithm	Encryption and decryption test	No
Abdelgader et al. (2015)	AES, IDEA and RSA	No performance evaluation	No

HYBRID SECURITY APPROACH IN INFORMATION SECURITY

With the advent of the IoT technology, numerous devices are getting connected to the Internet. As a result, information security is a crucial component in the design and development of all embedded devices. Researchers are aware of providing the best security practices in IoT devices for developing secure embedded applications. There are 11 articles that presented the hybrid approach in IoT information security. Li et al. (2017) proposed a new certificateless online/offline signcryption scheme and proved its security in the random oracle model. As compared with two existing certificateless online/offline signcryption schemes, the proposed scheme did not require any point multiplication operation in the online phase.

Several metrics were evaluated in the article such as the computation cost, security level (size of p and q), offline storage, ciphertext size and private key size. Fangfang, Huazhong, Dongqing and Yong (2013) introduced mixed encryption using symmetric DES and RSA public-key to further ensure message security while maintaining real-time performance. The effectiveness was proved by simulation for the GOOSE message of the substation's transmission with OPNET and the study also analyzed the delay of the encrypted message. Sujatha, Ramakrishnan, Duraipandian and Ramakrishnan (2015) developed a hybrid signcryption technique based on Key Encapsulation Mechanism (KEM) and Data Encapsulation Mechanism (DEM) techniques. KEM algorithm utilized KDF technique to encapsulate symmetric key. DEM algorithm utilized the Adaptive Genetic Algorithm based ECC algorithm to encrypt the original message. The proposed method outperformed existing techniques based on the encryption time, key similarity, key breaking time and computational time. Yousefi and Jameii (2017) proposed HAN algorithm combining AES symmetric and NTRU asymmetric algorithm.

The method was evaluated based on total speed time, total implementation time and percentage power usage. This proposed algorithm used less memory because of less fiscal complexity. Ravikant and Lilhore (2016) proposed new hybrid algorithms ElGamal-AES and Diffie-Hellman-AES to minimize decryption time. The hybrid D-AES and E-AES were more efficient compared to hybrid D-RSA, D-DES and D-TDES. The D-AES and E-AES decryption time was the fastest and more efficient with respect to security and key management. Bansod et al. (2015) proposed the hybrid cryptosystem, consisting of GRP and S-box of lightweight cipher PRESENT implementing on a 32-bit processor. This hybrid model resulted in 2125 gate equivalents, which was better than other light variant models like DESXL, CLEFIA, and AES. Narayanaswamy, Sampangi and Sampalli (2015) proposed hybrid algorithm requiring a simple XOR operation. The stream cipher approach was used to derive the key, while block cipher approach was adopted in the encryption process.

This proposal has successive key derivation function, which uses both a key as well as a message to choose the next key dynamically. Patil, Bansod and Pisharoty (2015) proposed a robust hybrid structure by fusion of RECTANGLE, LED and SPECK to improve the key scheduling aspect of LED and related key attacks. The hybrid cipher design was secure against linear and differential cryptanalysis. Mathur and Bansode (2016) proposed an extension of a public-key cryptosystem to support a private key cryptosystem using a combination of AES and ECC. The proposed method presented an overall security of the system by implementing software based countermeasures to prevent possible vulnerabilities e.g. timing and side channel attack. Arai and Obana (2016) proposed a new Password-Protected Secret Sharing (PPSS) model and scheme using Kurosawa-Desmedt hybrid

encryption that was proven to be CCA secure in the standard model. The proposed scheme was more secure than the Bagherzandi, Jarecki, Lu, and Saxena (2011) scheme with only the addition of a (about 160bit). Alkady, Habib and Rizk (2013) studied hybrid ECC and AES encryption algorithm, according to the characteristics of public key cryptography to secure file transfer system. The system guaranteed security of communication, ease of implementation, fast operation speed and low cost. Table 7 summarizes the related work in information security. Based on the table, it is found that some studies by Yousefi and Jameii (2017), Mathur and Bansode (2016), Ravikant and Lilhore (2016) and You et al. (2017) have implemented the AES scheme to protect data confidentiality in IoT information security.

Table 7

Hybrid Security Approach in Information Security Related-IoT

Study	**Method**	**Performance Metrics**	**Is security analysis/ proof presented?**
Li et al. (2017)	New Certificateless online/ offline signcryption scheme	Computation cost, security level (size of p and q), offline storage, ciphertext size, private key size	Yes
Fangfang et al. (2013)	DES and RSA	Delay of encrypted message	No
Sujatha et al. (2015)	KEM, DEM technique and Adaptive Genetic Algorithm based ECC	Encryption time, key similarity, key breaking, computation time	Yes
Yousefi and Jameii (2017)	AES and NTRU	Total speed time, total implementation time, percentage power usage	No
Ravikant et al. (2016)	ElGamal-AES and Diffie-Hellman-AES	Decryption time and key exchange time	No
Bansod et al. (2015)	GRP and S-box of lightweight cipher PRESENT	Memory size, gate count	Yes
Narayanaswamy et al. (2015)	Simple XOR operation, the block and stream cipher approach	Cryptanalysis	Yes
Patil et al. (2015)	RECTANGLE, LED and SPECK	Memory consumption, execution time, gate count, power calculation	Yes

(continued)

Study	Method	Performance Metrics	Is security analysis/ proof presented?
Mathur and Bansode (2016)	AES and ECC	Minimum number of active s-box, memory requirement, Gate Equivalent (GE), execution time	No
Arai and Obana (2016)	Kurosawa-Desmedt hybrid encryption	Computational cost	Yes
You et al. (2017)	ECC and AES	No performance evaluation	Yes

HYBRID SECURITY APPROACH IN SMART GRID

IoT offers several possibilities that can improve smart grid performance due to gathering data in real-time, creating more detailed analysis or automating some features. Nevertheless, it has to deal with numerous security solutions and economical aspects to become a mature, secure and ready-to-use technology. Four studies have presented the hybrid approach in IoT smart grid applications. Abbasinezhad-Mood and Nikooghadam (2018b) proposed an enhanced ECC based authentication and key agreement scheme. Based on the results of communication cost, computational cost and the execution time of different crypto algorithm, the hybrid technique was secure against well-known attacks and provided perfect forward secrecy. The same authors have also proposed ECC-based authentication and key agreement scheme consisting of three phases, namely ‘‘initialization’’, ‘‘registration’’, and ‘‘authentication’’ in Abbasinezhad-Mood and Nikooghadam (2018a).

The scheme has better efficiency than several other schemes in terms of performance in communication cost, computational cost and execution time of different crypto algorithms while providing more security features. Alharbi and Lin (2016) presented an efficient Identity Based Signcryption (EIBSC) scheme, composed mainly of four algorithms: system initialization algorithm, registration and private key extraction algorithm, signcryption algorithm, and unsigncryption algorithm. Privacy-preserving data was achieved in downlink communication from the control center to smart meter networks in residential areas. George, Nithin and Kottayil (2016) proposed a hybrid approach using public key (PKC) and symmetric key (SKE) for secure message exchange. The public and private key pairs were issued by Certificate Authority at the time of network establishment.

Using the approach, forward and backward secrecy was ensured; meeting confidentiality, authenticity and integrity requirements. The above-mentioned various hybrid approaches in smart grid applications are summarized in Table 8. Three of the studies evaluated communication and computation costs while a study by George et al. (2016) did not discuss performance evaluation or security analysis which could be because the paper was a framework study.

Table 8

Hybrid Security Approach in Smart Grid

Study	Method	Performance Metrics	Is security analysis/proof presented?
Abbasinezhad-Mood and Nikooghadam (2018b)	ECC based authentication and key agreement scheme	Communication cost, computational cost, execution time of different crypto algo	Yes
Alharbi and Lin (2016)	EIBSC scheme composed mainly of four algorithms: system initialization algorithm, registration and private key extraction algorithm, signcryption algorithm, and unsigncryption algorithm	Execution time, computation overhead, ciphertext size	Yes
Abbasinezhad-Mood and Nikooghadam (2018a)	ECC-based authentication and key agreement scheme	Communication cost, computational cost, execution time of different crypto algo	Yes
George, Nithin, and Kottayil (2016)	PKC and SKE	No performance evaluation	No

HYBRID SECURITY APPROACH IN FOG COMPUTING, BIOMETRIC AND SMART BANKING/E-COMMERCE FIELDS

Several studies have implemented the hybrid approach in fog computing, biometric and smart banking/e-commerce systems. These domains are also part of IoT applications which ultimately provides the full range of services to people everywhere based on the integration of applications. Only one paper was found to implement the hybrid technique in the area of fog computing. Lu, Heung, Lashkari and Ghorbani (2017) proposed a Lightweight Privacy-

preserving Data Aggregation (LPDA) scheme, characterized by employing homomorphic Paillier encryption, Chinese Remainder Theorem, and one-way hash. LPDA is very secure and privacy-enhanced with differential privacy techniques. In addition, the results of communication overhead and computational cost indicated that LPDA is lightweight in fog computing-enhanced IoT.

Also, two articles have developed the hybrid method in the biometric related-IoT field. Joshy and Jalaja (2017) presented a design and implementation of an embedded system for secure and reliable biometric authentication where the data was encrypted using hybrid encryption of Blowfish and RSA algorithm. The proposed two-step authentication provided high security to the system. Iovane, Bisogni, De Maio and Nappi (2018) presented hybrid information fusion algorithm, called Face Information Fusion (FIF) which was divided into three parts: face algorithm, RSA algorithm and FIF algorithm. The proposed algorithm could authenticate people easily.

Four articles presented the hybrid approach in smart banking and e-commerce systems. According to the approach by Kumar and Agarwal (2016), the hybrid system was divided into two: one was secure authentication and the other one was cost-effective encryption. This was achieved by using multi-factor authentications and ECC algorithm. The hybrid ECC consumed less bandwidth as well as less time as compared to hybrid RSA. Pourali, 2014 proposed the application of hybrid AES and ECC coding to secure data, which will be developed on SMS based model in electronic commerce. The approach provided secure payment through SMS which has all security specifications. Sharma and Bohra (2017) presented a hybrid approach using MD5 and RSA. It involved a five phase authentication system: User Id, User Password, User Unique Id, Match UID with QR code of user and a One Time Password. The author mentioned that the reason for implementing RSA was because the scheme was faster, and had simple encryption and verification processes. Solanki and Shiwani (2014) proposed an extremely large number that had two prime factors (similar to RSA). DES symmetric encryption was implemented to encrypt/decrypt data. It was clearly observable that the proposed method had a greater speed of transaction than conventional HTTPS. Table 9 summarizes the related work in fog computing, biometric and smart banking/e-commerce systems.

Table 9

Hybrid Security Approach in other Field related-IoT

Study	Method	Performance Metrics	Is security analysis/proof presented?
		Fog Computing	
Lu et al. (2017)	Homomorphic Paillier encryption, Chinese Remainder Theorem, and one-way hash function	Communication overhead and computational cost	Yes
		Biometric	
Joshy and Jalaja (2017)	Blowfish and RSA algorithm	Image test	No
Iovane et al. (2018)	Face algorithm, RSA algorithm and FIF algorithm	Frequency, cumulative sum, longest run	No
		Smart banking/E-commerce	
Kumar Choubey and Agarwal (2016)	Multi factor authentication and ECC and MA-RSA algorithm	Encryption and decryption time	Yes
Pourali (2014)	AES and ECC	No performance evaluation	Yes
Sharma and Bohra (2017)	MD5 and RSA	Encryption and decryption time	Yes
Solanki and Shiwani (2014)	RSA and DES	Http and https transaction time	No

DISCUSSION

Upon achieving the first objective, an overview of various hybrid security approaches is presented in this study. These approaches have been proposed by many researchers for implementation in IoT domains and applications. Based on Table 1 to Table 9, it can be concluded that the hybrid approach is mostly implemented in IoT cloud computing services. Most articles on hybrid security approaches in cloud computing did not present security analysis or mathematically proven methods. Most of the researchers only demonstrated the system model and web page development. Despite this, it was found that

the security analysis presented for multimedia data was based particularly on histogram analysis, adjacent correlation coefficient analysis and mean value analysis. Besides, this study has identified the performance metrics evaluated in each of the research work as a reference for other researchers in future work. It has also been found that some articles did not present performance analysis since their proposed work were preliminary studies, theories on security discussions, etc.

Meanwhile, the percentage of articles based on IoT components and applications is shown in a pie chart in Figure 1. It can be seen that publications related to Cloud computing produced the highest percentage of 19%, followed by 17% in the publication of multimedia data related-IoT and 16% for data transmission related-IoT. This result indicates that hybrid security in Cloud computing research forms a major part of IoT services. As reported by Jara, Genoud and Bocchi (2014), the IoT and Cloud have a complementary relationship. IoT generates massive amounts of data, while cloud computing provides a pathway for these data to travel. Thus this is the main reason why the hybrid techniques are proposed mostly in the Cloud services. Apart from this, the results have demonstrated the importance of securing data transmission and multimedia data due to the increasing number of IoT mobile device users year by year so as to prevent information leakage to untrusted participants.

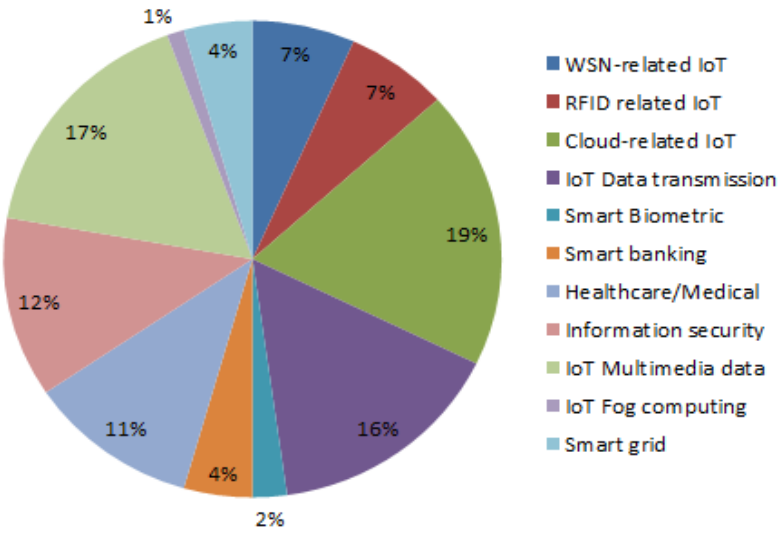

Figure 1. Percentage of reviewed papers based on IoT related fields.

Table 10 lists the number of publications which was produced yearly from 2013 to 2018. It can be seen that publications on the hybrid approach in IoT services had increased gradually, year by year. In addition, four articles published in 2018 were found to be related to hybrid cryptographic approaches. It is apparent from the table that this technique is going to grow with the increasing use of IoT technology in the near future.

Table 10

Number of Publications

Year	No. of Publications
2013	9
2014	7
2015	22
2016	23
2017	25
2018	4

The second objective has been achieved by identifying the most frequent algorithm used in the hybrid technique. Figures 2 and 3 present the well-known symmetric and asymmetric schemes employed in hybrid approaches. Figure 2 shows that the AES symmetric scheme is widely used in hybridization as reported in many publications in 2013 which is more than 50% of the total publications. However, the least frequent use of this scheme was in 2014. However, the AES implementation picked up from 2015 to 2017. This indicated that this scheme has become the most popular scheme in the hybrid technique since it has been used broadly in many publications. This concurred with the report by Singhal and Raina (2011), where most studies in AES found that this algorithm was fast in both software and hardware. Therefore it is efficient to be implemented in a wide range of platforms. For asymmetric encryption method, ECC was found to be the most popular among others. The advantage of the scheme is the high speed of computation and greater storage efficiency as reported by Abbasinezhad-Mood and Nikooghadam (2018a) which is why it was implemented extensively in hybrid cryptographic approaches from 2013 to 2018.

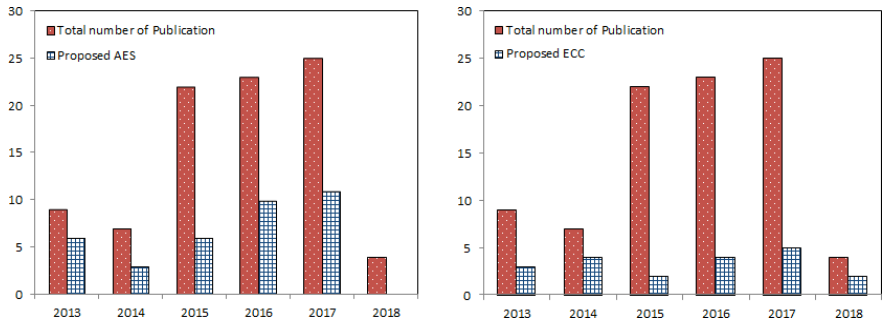

Figure 2. Total number of publications that proposed AES and ECC.

CONCLUSION

This literature study has reviewed the publications of the past 5 years in the search for hybrid cryptographic algorithms proposed in many IoT domains which may help researchers to orientate their research areas and choose the most feasible cryptographic schemes for their studies. A number of different useful techniques and algorithms have been prescribed in this paper that can be used for providing security in many IoT applications. The hybrid technique is a combination of several cryptographic algorithms which provides better security services compared to the conventional single method. The cryptographic methods and performance evaluation of many approaches were presented in the section under Review of Hybrid Cryptographic Approaches. It has been discovered from this review study, that the hybrid security approach is beneficial in securing numerous IoT services. Besides, it has been found that the hybridization technique is used in many IoT cloud domains which indicated that this technique is important to strengthen security in the cloud. In addition, computing speed and security resistance efficiency are the main reasons for the wide use of AES and ECC schemes in the hybridization technique. In future, we plan to review the security analysis methods used in studies to prove the security strength of hybrid cryptographic approaches.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education and the Research Management Institute, Universiti Teknologi MARA (UiTM)

for providing the BESTARI grant (600-IRMI/PERDANA 5/3 BESTARI [085/2018]), and the Faculty of Electrical Engineering, UiTM for the financial support in this research.

REFERENCES

Abbasinezhad-Mood, D., & Nikooghadam, M. (2018a). Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems*, *84*, 47–57. http://doi.org/10.1016/j.future.2018.02.034

Abbasinezhad-Mood, D., & Nikooghadam, M. (2018b). Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller. *Journal of Information Security and Applications*, *40*, 9–19. http://doi.org/10.1016/j.jisa.2018.02.007

Abdelgader, A. M. S., Wu, L., Simik, M. Y. E., & Abdelmutalab, A. (2015). Design of a secure file transfer system using hybrid encryption techniques. In *Proceedings of the World Congress on Engineering and Computer Science* (Vol. 2).

Adat, V., & Gupta, B. B. (2017). Security in Internet of things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423–441. http://doi.org/10.1007/s11235-017-0345-9

Al-Haj, A., Abandah, G., & Hussein, N. (2015). Crypto-based algorithms for secured medical image transmission. *IET Information Security*, *9*(6), 365–373. http://doi.org/10.1049/iet-ifs.2014.0245

Al-Haj, A., Hussein, N., & Abandah, G. (2016). *Combining cryptography and digital watermarking for secured transmission of medical images*. Proceedings of 2016 International Conference on Information Management, ICIM, 40–46. http://doi.org/10.1109/INFOMAN.2016.7477531

Alanazi, H. O., Zaidan, A. A., Zaidan, B. B., Kiah, M. L. M., & Al-Bakri, S. H. (2015). Meeting the security requirements of electronic medical records in the ERA of high-speed computing. *Journal of Medical Systems*, *39*(1), 9–12. http://doi.org/10.1007/s10916-014-0165-3

Alharbi, K., & Lin, X. (2016). *Efficient and privacy-preserving smart grid downlink communication using identity based signcryption*. http://doi.org/10.1109/GLOCOM.2016.7841770

Altigani, A., & Barry, B. (2013). *A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and word*

shift coding protocol. Proceedings - 2013 International Conference on Computer, Electrical and Electronics Engineering: "Research Makes a Difference", *ICCEEE*, 134–139. http://doi.org/10.1109/ICCEEE.2013.6633920

Arai, T., & Obana, S. (2016). *A password-protected secret sharing based on kurosawa-desmedt hybrid encryption*. Paper presented at the International Symposium on Computing and Networking (pp. 597–603). http://doi.org/10.1109/CANDAR.2016.86

Bagherzandi, A., Jarecki, S., Lu, Y., & Saxena, N. (2011). *Password-protected secret sharing password-protected secret sharing*. Paper presented at the ACM Conference on Computer and Communications Security (pp. 1–22). http://doi.org/10.1145/2046707.2046758

Bala, D. Q., Maity, S., & Jena, S. K. (2017). *A lightweight remote user authentication protocol for smart e-health networking environment*. Paper presented at the International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (pp. 10–15).

Bansal, V. P., & Singh, S. (2016). *A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs.* Paper presented at the 2nd International Conference on Recent Advances in Engineering and Computational Sciences, RAECS. http://doi.org/10.1109/RAECS.2015.7453367

Bansod, G., Raval, N., & Pisharoty, N. (2015). Implementation of a new lightweight encryption design for embedded security. *IEEE Transactions on Information Forensics and Security*, *10*(1), 142–151.

Belkaid, B. M., Mourad, L., Mehdi, C., & Soltane, A. (2015). Secure transfer of medical images using hybrid encryption. *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, *2*(2), 1–6.

Bhandari, A. (2016). *Secure algorithm for cloud computing and its applications*. Paper presented at the International Conference Cloud System and Big Data Engineering (pp. 188–192).

Bhave, A., & Jajoo, S. (2015). *Secure communication in wireless sensor networks using hybrid encryption scheme and cooperative diversity technique*. Paper presented at the IEEE Sponsored 9th International Conference on Intelligent Systems and Control.

Bisht, N., Thomas, J., & Thanikaiselvan. (2017). *Implementation of security algorithm for wireless sensor networks over multimedia images*. Paper presented at the International Conference onCommunication and Electronics Systems (ICCES).

Bouchti, A. El, Bahsani, S., & Nahhal, T. (2016). *Encryption as a service for data healthcare cloud security*. Paper presented at the 5th International Conference on Future Generation Communication Technologies*, FGCT*, 48–54. http://doi.org/10.1109/FGCT.2016.7605072

Bu, K., & Li, Y. (2018). Every step you take, i'll be watching you: Practical stepauth-entication of RFID paths. *IEEE Transactions on Information Forensics and Security*, *13*(4), 834–849. http://doi.org/10.1109/TIFS.2017.2768022

Chaturvedi, P., & Jain, D. C. (2016). *A hybrid RSA and RC6 based secure image cryptography to minimize entropy and enhance correlation*. Paper presented at the International Conference onApplied and Theoretical Computing and Communication Technology (pp. 32–37).

Chauhan, A., & Gupta, J. (2017). *A novel technique of cloud security based on hybrid encryption by blowfish and MD5*. Paper presented at the IEEE International Conference on Signal Processing, Computing and Control (pp. 349–355).

Cheon, J. H., & Kim, J. (2015). *A hybrid scheme of public-key encryption and somewhat homomorphic encryption*. IEEE Transactions on Information Forensics and Security, *10*(5), 1052–1063. http://doi.org/10.1109/TIFS.2015.2398359

D'souza, F. J., & Panchal, D. (2017). *Advanced encryption standard (AES) security enhancement using hybrid approach*. Paper presented at the International Conference on Computing, Communication and Automation (pp. 647–652).

Dahiya, S., & Bohra, M. (2017). *Hybrid parallel partial model for robust & secure authentication in healthcare IoT environments*. Paper presented at the IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON) (pp. 239–243). http://doi.org/10.1109/UPCON.2017.8251054

Dawahdeh, Z. E., Yaakob, S. N., & Razif Othman, R. (2017). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University - Computer and Information Sciences*, 0–6. http://doi.org/10.1016/j.jksuci.2017.06.004

Fangfang, W., Huazhong, W., Dongqing, C., & Yong, P. (2013). Substation communication security research based on hybrid encryption of des and RSA. *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP, 437–441. http://doi.org/10.1109/IIH-MSP.2013.115

Fei, X., Li, K., Yang, W., & Li, K. (2016). A secure and efficient file protecting system based on SHA3 and parallel AES. *Parallel Computing*, *52*, 106–132. http://doi.org/10.1016/j.parco.2016.01.001

Gajra, N., Khan, S. S., & Rane, P. (2014). *Private cloud security : Secured user authentication by using enhanced hybrid algorithm*. Paper presented at the International Conference on Advances in Communication and Computing Technologies Private (pp. 1–6).

Gallagher, P. (2012). Secure hash standard (SHS) FIPS PUB 180-4. *Processing*, *FIPS PUB 1*(October).

George, N., Nithin, S., & Kottayil, S. K. (2016). Hybrid key management scheme for secure AMI communications. *Procedia Computer Science*, *93*(September), 862–869. http://doi.org/10.1016/j.procs.2016.07.260

Gonçalves, R., Leonova, E., Puttini, R., & Nascimento, A. (2015). A privacy-ensuring scheme for health data outsourcing. *Proceedings of 2015 International Conference on Cloud Computing Technologies and Applications, CloudTech*. http://doi.org/10.1109/CloudTech.2015.7336982

Goyal, K., & Kinger, S. (2013). Hybrid approach using encryption algorithms for data storage. *International Journal of Scientific & Engineering Research*, *4*(7), 2063–2067.

Gupta, S., Kalra, A., & Hasti, C. (2016). *A hybrid technique for spatial image steganography*. Paper presented at the 3rd International Conference onComputing for Sustainable Global Development (INDIACom) (pp. 643–647).

Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. *Engineering, Technology & Applied Science Research*, *7*(4), 1781–1785.

Hong, N., & Xuefeng, Z. (2013). A security framework for Internet of things based on SM2 cipher algorithm. *International Conference on Computational and Information Sciences*, 13–16. http://doi.org/10.1109/ICCIS.2013.12

Hong, Z.-Y., Qiu, Z.-P., Zeng, S.-L., Wang, S.-D., & Sandrine, M. (2017). *Research on fusion encryption algorithm for Internet of things monitoring equipment*. Paper presented at the International Symposium on Pervasive Systems, Algorithms and Networks & nternational Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (pp. 425–429). http://doi.org/10.1109/ISPAN-FCST-ISCC.2017.49

Iovane, G., Bisogni, C., De Maio, L., & Nappi, M. (2018). An encryption approach using information fusion techniques involving prime numbers and face biometrics. *IEEE Transactions on Sustainable Computing*, *3782*, 1–11. http://doi.org/10.1109/TSUSC.2018.2793466

Iyer, S. C., Sedamkar, R. R., & Gupta, S. (2016). Anovel idea on multimedia encryption using hybrid crypto approach. *Procedia Computer Science*, *79*, 293–298. http://doi.org/10.1016/j.procs.2016.03.038

Jeddi, Z., Amini, E., & Bayoumi, M. (2013). *A novel authenticated encryption algorithm for RFID systems*. Paper presented at the Euromicro Conference on Digital System Design (pp. 658–661). http://doi.org/10.1109/DSD.2013.117

Joshy, A., & Jalaja, M. J. (2017). *Design and implementation of an IoT based secure biometric authentication system*. Paper presented at the

IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), 1–13. http://doi.org/10.1109/SPICES.2017.8091360

Kanna, G. P., & Vasudevan, V. (2016). *Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud*. Paper presented at the International Conference on Electrical, Electronics, and Optimization Techniques (pp. 3688–3693). http://doi.org/10.1109/ICEEOT.2016.7755398

Kaur, A., & Singh, S. (2016). *A hybrid technique of cryptography and watermarking for data encryption and decryption*. Paper presented at the Fourth International Conference on Parallel, Distributed and Grid Computing.

Kaushik, S., & Gandhi, C. (2016). *Cloud data security with hybrid symmetric encryption***.** Paper presented at the International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT- Proceedings, 636–640. http://doi.org/10.1109/ICCTICT.2016.7514656

Kavitha, R. J., & Caroline, B. E. (2015). *Hybrid cryptographic technique for heterogeneous wireless sensor networks*. Paper presented at the International Conference on Communications and Signal Processing (ICCSP) (pp. 1016–1020). http://doi.org/10.1109/ICCSP.2015.7322653

Kessler, G. C. (1998). An overview of cryptography. In *Handbook on Local Area Network* (pp. 1–63). http://doi.org/10.4018/978-1-4666-3685-9.ch006

Kester, Q. A., Nana, L., Pascu, A. C., & Gire, S. (2013). A new encryption cipher for securing digital images of video surveillance devices using Diffie-HellMan-MD5 algorithm and RGB pixel shuffling. In *European Modelling Symposium on Computer Modelling and Simulation* (pp. 305–311). http://doi.org/10.1109/EMS.2013.53

Kester, Q., Nana, L., & Pascu, A. C. (2013). *A new hybrid asymmetric key-exchange and visual cryptographic algorithm tor securing digital images*. Paper presented at the International Conference on Adaptive Science and Technology (ICAST).

Kirichek, R., Kulik, V., & Koucheryavy, A. (2016). *False clouds for Internet of things and methods of protection*. Paper presented at the International Conference on Advanced Communication Technology, ICACT, 201–205. http://doi.org/10.1109/ICACT.2016.7423328

Kotel, S., Sbiaa, F., Zeghid, M., Machhout, M., Baganne, A., & Tourki, R. (2016). *Efficient hybrid encryption system based on block cipher and chaos generator*. Paper presented at the IEEE International Conference on Computer and Information Technology (CIT), *1*, 375–382. http://doi.org/10.1109/CIT.2016.45

Kumar Choubey, S., & Agarwal, A. (2016). *Improving banking authentication using hybrid cryptographic technique.* Paper presented at the IEEE International Conference on Computer Communication and Control, IC4. http://doi.org/10.1109/IC4.2015.7375511

Li, F., Han, Y., & Jin, C. (2017). Certificateless online/offline signcryption for the Internet of things**.** *Wireless Networks***,** *23*(1), 145–158. http://doi.org/10.1007/s11276-015-1145-3

Lin, S., Zhang, R., Ma, H., & Wang, M. (2015). Revisiting attribute-based encryption with verifiable outsourced decryption. *IEEE Transactions on Information Forensics and Security*, *10*(10), 2119–2130. http://doi.org/10.1109/TIFS.2015.2449264

Lin, Y., Kang, K., & Shi, Y. (2013). *Research on encryption model based on AES and ECC in RFID.* Paper presented at the International Conference on Computer Sciences and Applications, CSA 2013 (pp. 9–13). http://doi.org/10.1109/CSA.2013.10

Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). *A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT*. IEEE Access, *5*, 3302–3312. http://doi.org/10.1109/ACCESS.2017.2677520

Ma, L., & Jin, W. (2018). Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer generated holography. *Optics Communications***,** *407***,** 51–56. http://doi.org/10.1016/j. optcom. 2017.08.047

Mahalle, V. S., & Shahade, A. K. (2014). *Enhancing the data security in cloud by implementing hybrid (Rsa & Aes) encryption algorithm*. Paper presented at the International Conference on Power, Automation and Communication, INPAC, (1), 146–149. http://doi.org/10.1109/INPAC.2014.6981152

Maitri, P. V., & Verma, A. (2016). *Secure file storage in cloud computing using hybrid cryptography algorithm.* Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET, 1635–1638. http://doi.org/10.1109/WiSPNET.2016.7566416

Manjula, Y., & Shivakumar, K. B. (2016). *Enhanced secure image steganography using double encryption algorithms.* Paper presented at the Computing for Sustainable Global Development (INDIACom), 3rd International Conference On, *7*, 705–708.

Mathur, N., & Bansode, R. (2016). AES based text encryption using 12 rounds with dynamic key selection. *Procedia Computer Science***,** *79*, 1036–1043. http://doi.org/10.1016/j.procs.2016.03.131

Moon, P. S., & Ingole, P. K. (2015). *An overview on*: *Intrusion detection system with secure hybrid mechanism in wireless sensor network*. Paper

presented at the International Conference on Advances in Computer Engineering and Applications (pp. 272–277). http://doi.org/10.1109/ICACEA.2015.7164714

Narayanaswamy, J., Sampangi, R. V., & Sampalli, S. (2015). *HIDE: Hybrid symmetric key algorithm for integrity check, dynamic key generation and encryption*. International Conference Information Systems Security and Privacy (ICISSP), 124–131.

Olumide, A., Alsadoon, A., Prasad, P. W. C., & Pham, L. (2015). *A hybrid encryption model for secure cloud computing*. Paper presented at the International Conference on ICT and Knowledge Engineering (pp. 24–32). http://doi.org/10.1109/ICTKE.2015.7368466

Patil, A., Bansod, G., & Pisharoty, N. (2015). Hybrid lightweight and robust encryption design for security in IoT. *International Journal of Security and Its Applications*, *9*(12), 85–98. http://doi.org/10.14257/ijsia.2015.9.12.10

Poornima, B., & Rajendran, T. (2014). *Improving cloud security by enhanced HASBE using hybrid encryption scheme*. Proceedings - World Congress on Computing and Communication Technologies*, WCCCT*, 312–314. http://doi.org/10.1109/WCCCT.2014.88

Pourali, A. (2014). *The presentation of an ideal safe SMS based model in mobile electronic commerce using encryption hybrid algorithms AES and ECC.* Paper presented at the International Conference on E-Commerce in Developing Countries: With Focus on e-Trust. http://doi.org/10.1109/ECDC.2014.6836761

Purevjav, S., Kim, T., & Lee, H. (2016). Email encryption using hybrid cryptosystem based on android, 968650.

Qi, J., Hu, X., Ma, Y., & Sun, Y. (2015). *A hybrid security and compressive sensing-based sensor data gathering scheme*. IEEE Access, *3*, 718–724. http://doi.org/10.1109/ACCESS.2015.2439034

Qiu, Y., Ma, M., & Chen, S. (2017). An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems. *Computer Networks***.** http://doi.org/10.1016/j.comnet.2017.10.006

Ramesh, A., & Jain, A. (2015). *Hybrid image encryption using pseudo random number generators, and transposition and substitution techniques*. Paper presented at the International Conference on Trends in Automation, Communications and Computing Technology.

Ravikant, K., & Lilhore, U. K. (2016). *Combined cryptographic standards for minimizing the decryption time of encrypted data using E-AES and D-AES*. Paper presented at the International Journal of Innovative Research in Computer and Communication Engineering, *4*(11), 19783–19788.

Rizk, R., & Alkady, Y. (2015). Two-phase hybrid cryptography algorithm for wireless sensor networks. *Journal of Electrical Systems and Information Technology*, *2*(3), 296–313. http://doi.org/10.1016/j.jesit.2015.11.005

Saini, J. K., & Verma, H. K. (2013). *A hybrid approach for image security by combining encryption and steganography*. Paper presented at the IEEE 2nd International Conference on Image Information Processing, IEEE ICIIP, 607–611. http://doi.org/10.1109/ICIIP.2013.6707665

Saleh, M. E.,Aly,A.A., & Omara, F.A. (2016). Data security using cryptography and steganography. *International Journal of Advanced Computer Science and Applications*, *7*(6), 39–397. http://doi.org/10.9790/0661-180405130139

Sengupta, N., & Chinnasamy, R. (2015). Contriving hybrid DESCAST algorithm for cloud security. *Procedia Computer Science***,** *54*, 47–56. http://doi.org/10.1016/j.procs.2015.06.006

Sharma, A., & Singh, A. (2017). *Hybrid improved technique for data security and authentication for RFID tags.* Paper presented at the 4th International Conference on Signal Processing, Computing and Control (ISPCC), (pp. 536–540).

Sharma, N., & Bohra, B. (2017). *Enhancing online banking authentication using hybrid cryptographic method security issues in online banking application.* Paper presented at the IEEE International Conference on Computational Intelligence and Communication Technology (pp. 1–8). http://doi.org/10.1109/CIACT.2017.7977275

Sharma, R., & Joshi, B. (2017). H-IBE: *Hybrid-identity based encryption approach for cloud security with outsourced revocation*. Paper presented at the International Conference on Signal Processing, Communication, Power and Embedded System (pp. 1192–1196). http://doi.org/10.1109/SCOPES.2016.7955629

Sharma, S., & Chopra, V. (2017). Data encryption using advanced encryption standard with key generation by Elliptic Curve Diffie-Hellman. *International Journal of Security and Its Applications*, *11*(3), 17–28.

Singh, R., Panchbhaiya, I., Pandey, A., & Goudar, R. H. (2015). Hybrid Encryption Scheme (HES): An approach for transmitting secure data over Internet. *Procedia - Procedia Computer Science***,** *48*(Iccc), 51–57. http://doi.org/10.1016/j.procs.2015.04.109

Singhal, N., & Raina, J. P. S. (2011). Comparative analysis of AES and RC4 algorithms for better utilization. *International Journal of Computer Trends and Technology*, 177–181. http://doi.org/2231-280

Smithamol, B., & Rajeswari, S. (2017). Hybrid solution for privacy - preserving access control for healthcare data. *Advances in Electrical and Computer Engineering*, *17*(2), 31–38. http://doi.org/10.4316/AECE.2017.02005

Solanki, D. S., & Shiwani, S. (2014). *A model to secure e-commerce transaction using hybrid encryption*. Paper presented at the International Conference on Control, Instrumentation, Communication

and Computational Technologies, ICCICCT, 642–645. http://doi.org/10.1109/ ICCICCT.2014.6993040

Sridhar C Iyer, Sedamkar, R. ., & Gupta, S. (2016). A Novel Idea of Video Encryption using Hybrid Cryptographic Techniques. In *International Conference on Inventive Computation Technologies* (pp. 1–5).

Sujatha, R., Ramakrishnan, M., Duraipandian, N., & Ramakrishnan, B. (2015). Optimal adaptive genetic algorithm based hybrid signcryption algorithm for information security. *CMES - Computer Modeling in Engineering and Sciences*, *105*(1), 47–68.

Sujithra, M., Padmavathi, G., & Narayanan, S. (2014). Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud. P*rocedia Computer Science***,** *47*(C), 480–485. http://doi.org/10.1016/j.procs.2015.03.232

Xin, M. (2015). A *mixed encryption algorithm used in Internet of things security transmission system.* Paper presented at the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (pp. 62–65). http://doi.org/10.1109/CyberC.2015.9

Yin, A., & Liang, H. (2014). Certificateless Hybrid Signcryption Scheme for Secure Communication of Wireless Sensor Networks. *Wirel. Pers. Commun.***,** *80*(3), 1049–1062. http://doi.org/10.1007/s11277-014-2070-y

You, W., Shi, G., Chen, X., Qi, J., & Qing, C. (2017). Research on a hybrid system with perfect forward secrecy. In *IEEE Information Technology, Networking, Electronic and Automation Control Conference* (pp. 1783–1787).

Yousefi, A., & Jameii, S. M. (2017). Improving the security of the Internet of things using encrypted algorithms. *International Journal of Computer and Information Engineering*, *11*(5), 3–7.

Zakir, M., & Sarker, H. (2005). A cost effective symmetric key cryptographic algorithm for small amount of data. Paper presented at the IEEE International Multitopic Conference (pp. 1–6).

Zhai, X., Ait Si Ali, A., Amira, A., & Bensaali, F. (2017). ECG encryption and identification based security solution on the Zynq SoC for connected health systems. J*ournal of Parallel and Distributed Computing***,** *106***,** 143–152. http://doi.org/10.1016/j.jpdc.2016.12.016

Zhang, Y., Zheng, D., Chen, X., Li, J., & Li, H. (2016). Efficient attribute-based data sharing in mobile clouds. *Pervasive and Mobile Computing***,** *28*, 135–149. http://doi.org/10.1016/j.pmcj.2015.06.009

Zhao, T., Ran, Q., & Chi, Y. (2015). Image encryption based on nonlinear encryption system and public-key cryptography. *Optics Communications***,** *338*, 64–72. http://doi.org/10.1016/j.optcom.2014.09.083

Zhong, H., Shao, L., Cui, J., & Xu, Y. (2018). An efficient and secure recoverable data aggregation scheme for heterogeneous wireless sensor networks. *J. Parallel Distrib. Comput.***,** *111*, 1–12. http://doi. org/10.1016/j.jpdc.2017.06.019