A New Hybrid Cryptosystem for Internet of Things Applications

Ashraf Darwish, Maged M. El-Gendy and Aboul Ella Hassanien

Abstract The Internet of Things or ‘‘IoT’’ defines a highly interconnected network of heterogeneous devices where all kinds of communications seem to be possible. As a result, the security requirement for such network becomes critical whilst these devices are connected. Today, all commercial applications will be performed via Internet; even the office environment is now extending to employ’s home. This chapter presents a new proposed cyber security scheme for IoT to facilitate additional level of security through the involvement of a new level of key-hierarchy. In this chapter, we present the closed system environment, the proposed scheme, the services provided, the exchange of message format, and the employed four level key-hierarchies. We use application level security for selectively securing information to conserve power and increase computational speed which is useful for IoT and wireless applications. The analysis of the proposed scheme is discussed based on the strength of symmetric algorithms such as RSA and AES algorithms.

Keywords Cryptography · Cyber security · Hybrid cryptosystems · One-time pad · Internet of things (IoT)

1 Introduction

The main objective of cryptography is to allow users to communicate in a secure way over the Internet network. Cryptography is considered as two categories: symmetric key cryptography as described in [1–4] and public key-cryptography infrastructure (PKI) [5–7]. Both symmetric key and PKI possess the necessary

A. Darwish (✉) · M.M. El-Gendy
Faculty of Science, Computer Science Department, Helwan University,
Cairo, Egypt
e-mail: ashraf.darwish.eg@ieee.org; mmostafa_fouad@yahoo.com

A.E. Hassanien
Faculty of Computers and Information, Cairo University, Cairo, Egypt
e-mail: aboitcairo@gmail.com

A.E. Hassanien et al. (eds.), *Multimedia Forensics and Security*,
Intelligent Systems Reference Library 115, DOI 10.1007/978-3-319-44270-9_16

characteristics to information security for a wide variety of applications such as electronic commerce, e-mail, e-voting systems via Internet, cloud computing, and IoT future applications.

There are four basic categories of attacks are described in [8]: (i) data disclosure, (ii) Fraud, (iii) data insertion, (iv) removal, and modification, and denial of service. Several security techniques and services are introduced in [9] to protect the mentioned threats which identified above as: authentication, access control, integrity, and privacy.

For some sensitive applications such as military applications, diplomatic communications, electronic commerce or electronic cash applications, the exchange of information through the Internet represents a sever vulnerability to such systems [10]. That is why we are in need to a secure cryptographic environment that supports a cryptographic technique that is proved to be very hard to break, through a closed system (business-to-; business connection).

Therefore, we demonstrate, in this chapter that represents an extended version [11], a new proposed unconditionally secure hybrid cryptosystem. This system is working in an environment that represents a closed system (business-to-business connection) by constructing an extranet connected over a VPN, through the tunneling technology and the e-mail exchange secure messages. The combination of the one-time pad with the RSA and AES cryptosystems, improves the one-time pad key management through the washing process. The proposed scheme provides four levels; of key-hierarchy. The first is the one-time pad key. It is used to encrypt the message after the washing process. The second is the AES session key that is used in the washing process. The third is the RSA public key, which is used to encrypt the AES session keys and the OTP pointer. The fourth is the pass phrase used to protect the encryption of the private keys. The proposed cryptosystem combines the one-time pad, known as Vernam cipher, which is theoretically unbreakable cipher, with the standard encryption algorithms, the RSA public-key algorithm, and the AES secret-key algorithm.

The one-time pad, under the assumption that it has been shared and exchanged between the users securely offers unbreakable cipher. The strength of the proposed cryptosystem will be formulated and presented. Hybrid systems are introduced in the literature based on the integration of the benefits of the symmetric and the asymmetric cryptosystems. There are public key algorithms have been presented in the literature that can provide authentication, and data integrity. Public key algorithms are computationally complex by their nature. These algorithms are known hash functions [12–15]. The Digital Signature Standard (DSS) [10, 16] can be applied in digital signature. Hybrid systems standards have been developed in the research for the exchange of encrypted data such as e-mails, including those for Privacy Enhanced Mail (PEM) [2], Pretty Good Privacy (PGP) [8], and Multipurpose Internet Mail Extensions (S/MIME).

This chapter establishes a secure cryptographic environment to sensitive applications such that their users can communicate securely, comfortably, and fast. Under this closed system environment, we are in need to a cryptosystem that achieve an ultimate security. With respect to matters related to the IoT management, it is not clear how this problem will be resolved in the context of this technology; however the distributed IoT technology can provide some solutions. Moreover, it will be difficult to retrieve all the relevant information throughout the network that might be needed for forensic analysis [17].

The rest of this paper is organized as follows. Section 2 introduces the related research work. Section 3 explores in details the proposed scheme. Section 4 describes the results and analysis of the proposed framework. A conclusion is presented in Sect. 5.

2 Related Work

A PKI algorithm allows client-server application to get trust in each other's authentication credentials in an efficient way. Hybrid cryptography systems can employ those credentials to improve authentication and make use of end-to-end confidentiality and integrity services. This public key functionality can enable a secure e-mail service, secure Web browsing, secure data storage, and secure networking.

A certificate is a statement issued by an authority of certification, according to a policy that binds an entity's public key to its name for a period of time. Entities can get private-public key pairs with associated public key certificates.

RSA algorithms are asymmetric cryptographic which encrypt symmetric keys in key exchange protocols and in hybrid cryptographic systems. In addition, entities X and Y can use end-to-end integrity services and confidentiality without the cooperation of any third entity.

Chatterjee [18] introduced a new method of combined cryptographic. In this paper, authors Vernam Cipher Method has been modified the standard for all characters (ASCII code 0-255) with randomized keypad, and introduced a feedback mechanism.

In [19], the Baek presented a hybrid identity-based encryption system which produce compact cipher texts while providing both efficiency and security. Baek provides a security analysis of Presented schemes against chosen cipher text attack under the well-known computational assumptions in the random oracle model.

There is computational soundness result for key exchange protocols with symmetric encryption has been presented in [20] by applying the lines of a chapter by Canetti and Herzog on protocols with public-key encryption.

Kusters [21], proposed a fully an encryption scheme. Kusters introduced a PKI scheme by using ideal lattices. The results of the proposed scheme in this paper are showed this scheme is simple and easy to be implemented for shadow images. In addition, this scheme can be applied in many electronic business areas.

Gentry [22] designed a hierarchical key assignment schemes which are secure and efficient. The Gentry applied two different constructions for time-bound hierarchical key assignment systems.

With the necessity need to store massive data in cyberspace and cross platforms, a certain security requirements must be met to efficiently protect confidentiality and privacy and this mechanism has been introduced in [23]. In this chapter, the authors review the state;-of-the-art of hybrid cryptosystems. Then, a novel scheme has been proposed for lightweight encryption of bulk data based on recursive cryptographic hashes and dynamic keys.

Nishanth [24] introduces SwiftEnc, a lightweight hybrid system that can be used effectively to encrypt bulk data. The main aim of this work was to produce a cipher text in a faster time than those of asymmetric algorithms.

A hybrid cryptography approach with the specification of two geometrical shapes i.e. ellipse and the rectangle has been presented in [25]. Two geographical shapes are taken as the cover to place the information and the series of geometric transformation operations are defined to encode the information, which uses the properties of ellipse, rectangle and symmetric-key algorithm, the algorithm is based on 2-d geometry using property of ellipse and rectangle. The work includes hybrid geometric shapes and alternative transformation so that more information security will be achieved. Also the work includes dynamic generation of key; it will provide more robustness against information size.

E-commerce is a prominent field in the future of business and security in e-commerce is becoming an important issue to transfer business from physical online stores [26]. Both protecting payment web application users and application systems need an integration of, technical, managerial, and physical controls. This chapter proposed a hybrid cryptographic system that combines both RSA and symmetric key algorithms.

In [27] Saeed and Al-Khalidi presented a new post-quantum unconditionally hiding commitment system which can support zero-knowledge protocols and allow to refresh the binding property over time. The design of the proposed system relies on the approximate shortest vector problem and lattice problem. Nguyen et al. [28] presented a new hybrid system whose bendiness relies on the discrete logarithm and approximate shortest vector problems.

A new hybrid crypto concept is proposed which is the combination of new symmetric and message digesting function (MD-5) has been presented in [29]. Moreover, the security and performance of the proposed technique are calculated and the presented results showing the performance of the proposed technique. In [30], the proposed architecture integrates the cryptographic algorithms, Advanced Encryption Standard algorithm (Symmetric) and the Hash function, SHA-2 to improve the data security to a greater extent.

3 Demonstration of a New Hybrid Scheme

Security is an important issue for communication via communication networks. With the increasing use of the Internet, the need of authentication and unconditionally secure encryption schemes is an important issue. Many governmental and commercial organizations are no longer willing to send their important information unencrypted over an the Internet network.

1. Target Objective

The main objective is to establish a secure cryptographic environment to sensitive applications such that their users can communicate securely, comfortably, and fast. Under this closed system environment, we are in need to a cryptosystem that achieve an ultimate security. We propose a cryptographic architecture that provides the following advantages:

(a) Using the tunneling technology to build the VPN (closed system) will enable using the infrastructure of the Internet. Tunneling makes extranet subscribers connectivity a viable option.
(b) An ultimate securely cryptosystem that provides the confidentiality, authentication, and data integrity.

2. Proposed Scheme Demonstration

Hybrid systems are based on the integration of the features of both the symmetric and the asymmetric cryptosystems. Furthermore, in our Proposed Hybrid scheme, the one-time pad cipher is applied. Therefore, we can explain the two main cycles of the scheme as follows:

(a) Sending Cycle
    i. *Washing Process*: In which, we wash (encrypt) the one-time pad key portion using AES algorithm and a cryptographic random session key using *ANSI X9.17* standard generator.
    ii. *Key Exchange Process*: In which, we encrypt the AES session key using the RSA public-key algorithm.
    iii. *Digital Envelope Process*: In which, we encrypt the message (file) with OTP, and complete our message formatting to be ready to transmit to the receiver supported with electronic digital signature of the sender.

(b) Receiving Cycle
    i. *Key Extraction Process*: In which, we extract the encrypted AES session key using the RSA public-key algorithm.
    ii. *Washing Process*: In which, we wash (encrypt) the one-time pad key portion using AES algorithm and the extracted AES session key.
    iii. *Digital Envelope Opening Process*: In which, we open our message to extract the different message segments. We decrypt the receiving message (file) and validate the digital signature of the sender and the integrity of the message.

3. Terminology Applied During the Demonstration

The following terminologies shown in Table 1 can be applied throughout the demonstration of our proposed scheme.

Table 1 The terminology applied

Terminology	Meaning
M, C	The plaintext and ciphertext messages
OTP_e	The washed one–time pad
AES^{-1}	AES decryption algorithm
Kid	The 256–bit AES session key
RSA^{-1}	RSA decryption algorithm
KR, KP	The RSA private and public keys
KRA, KPA	The private and public keys of the sender A
KRB, KPB	The private and public keys of the receiver B
SHA	The secure algorithm SHA-1
SIG	The signature (message digest encrypted by KRA)
CK	The Kid and the Scheme Pointers encrypted by the KPB
Env	The resulting digital envelope
$\text{Digest}_{r,}$ Digest_g	The received and generated digest respectively
+ ⊕	Concatenation and Vector sum modulo two operation

4. Operational Description

The Proposed Hybrid scheme provides confidentiality and authentication that can be used for the Internet sensitive applications and file storage.

(a) Authentication

In our scheme we use the Secure Hash Algorithm (SHA-1) to calculate the fingerprint of the message [15]. Figure 1 depicts the digital signature which provided by the proposed system. The *SHA-1* and *RSA* are used to provide a secure digital signature system. The formulation of the authentication process in the scheme is as follows:

(i) sending cycle:

$$\begin{aligned} SIG &= RSA_{KRA}(SHA\,[M]) \\ Env &= M + SIG \end{aligned}$$

(ii) receiving cycle: to validate the sender and the integrity of the received message:

$$\begin{aligned} Env &= M + SIG \\ Digest_g &= SHA\,[M] \ldots \textit{generated by the receiver} \\ Digest_r &= RSA^{-1}_{KPA}[SIG] \\ &= RSA^{-1}_{KPA}(RSA_{KRA}[SHA[M]) \\ &= SHA[M] \end{aligned}$$

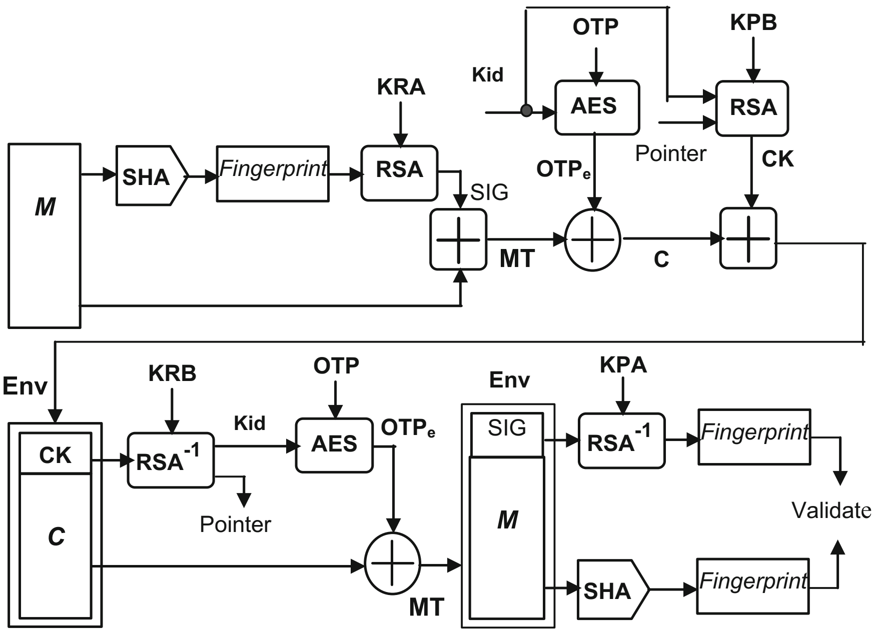

Fig. 1 Authentication and confidentiality

(b) Confidentiality

In the proposed system in this paper, the massage has been encrypted by using the OTP string as a key with a length equal to the message length, using the vector sum modulo two operations. The receiver has the same copy of the OTP that he can use it to decrypt the received message after washing the OTP key portion. The AES session key is recovered by the RSA receiver's private key after striping it off from the message then used it in washing process. The formulation of the confidentiality is as follows:

(i) Sending cycle

1. Washing Process:

$$OTP_e = AES_{kid}[OTP]$$

2. Key Exchange Process:

$$CK = RSA_{KPB}[kid + Pointer]$$

3. Digital Envelope Process:

$$\begin{aligned} C &= M \oplus OTP_e \\ Env &= C + CK \\ &= (M \oplus OTP_e) + (RSA_{KPB}[kid + Pointer]) \end{aligned}$$

(ii) Receiving cycle

1. Session Key Extraction Process:

$$Kid + Pointer = RSA^{-1}_{KRB}[CK]$$

2. Washing Process:

$$OTP_e = AES_{kid}[OTP]$$

3. Digital Envelope Opining Process:

$$M = C \oplus OTP_e = [M \oplus OTP_e] \oplus OTP_e$$

(c) Confidentiality and Authentication

Both confidentiality and authentication [31] can be applied to the same message. First, the signature of a message M is generated and appended to M. The OTP key is selected and washed using AES algorithm. Both the message and the signature together are encrypted with OTP$_e$ using the vector sum modulo two operations to generate the encrypted message C. The session key, kid, and the OTP pointer are encrypted using RSA and sent with C in a special formatting. The formulation of the confidentiality and the authentication is as follows:

(i) Sending cycle

1. Washing Process:

$$OTP_e = AES_{kid}[OTP]$$

2. Key Exchange Process:

$$CK = RSA_{KPB}[kid + Pointers]$$

3. Digital Envelope Process:

$$\begin{aligned} SIG &= RSA_{KRA}(SHA[M]) \\ MT &= M + SIG \\ C &= OTP_e \oplus MT = OTP_e \oplus [M + SIG] \\ &= OTP_e \oplus (M + RSA_{KRA}(SHA[M])) \\ Env &= C + CK \end{aligned}$$

(ii) Receiving cycle

1. Session Key Extraction Process:

$$Kid = RSA_{KRB}^{-1}[CK]$$

2. Washing Process:

$$OTP_e = AES_{kid}[OTP]$$

3. Digital Envelope Opening Process:

$$\begin{aligned} MT &= C \oplus OTP_e = (OTP_e \oplus (M + SIG)) \oplus OTP_e \\ &= M + SIG = M + RSA_{KRA}(SHA[M]) \\ Digest_g &= SHA[M] \;\ldots generated\, by\, the\, receiver \\ Digest_r &= RSA_{KPA}^{-1}[SIG] = RSA_{KPA}^{-1}(RSA_{KRA}[SHA[M]) \\ &= SHA[M]. \end{aligned}$$

Then, the two fingerprints, $Digest_g$ and the $Digest_r$, are compared for matching to validate the sender and the integration of the received message.

Before using OTP to encrypt the message, the OTP string is encrypted through the washing process using AES algorithm with a random 256–bit session key. Each OTP key and session key is used only once for each massage. To protect the used session key, it is encrypted with the RSA receiver's public key, and sent together with the encrypted massage.

(d) Transmitted Message Format

Figure 2 illustrates the transmitted message formatting, which yields the following segments:

(i) Multicasting Segment: It includes one entry for each recipient. The sender may broadcast the message to all the recipients or multicast some recipients. It includes:

- The identifier of the receiver public key, SHA (KPB) that was used by the sender to encrypt the AES session key. One entry for each recipient.
- The AES session key and the OTP pointer, encrypted by the receiver public key, KPB (Kid, Offset, Length). One entry for each recipient. The OTP pointer is composed of The starting offset of the OTP, from which an OTP string is used to encrypt the message and The length of the used OTP portion,
- The identifier of the sender public key, SHA (KPA), for which the corresponding private key was used to encrypt the message digest. Again, the public-key identifier is the SHA hash code of the key.

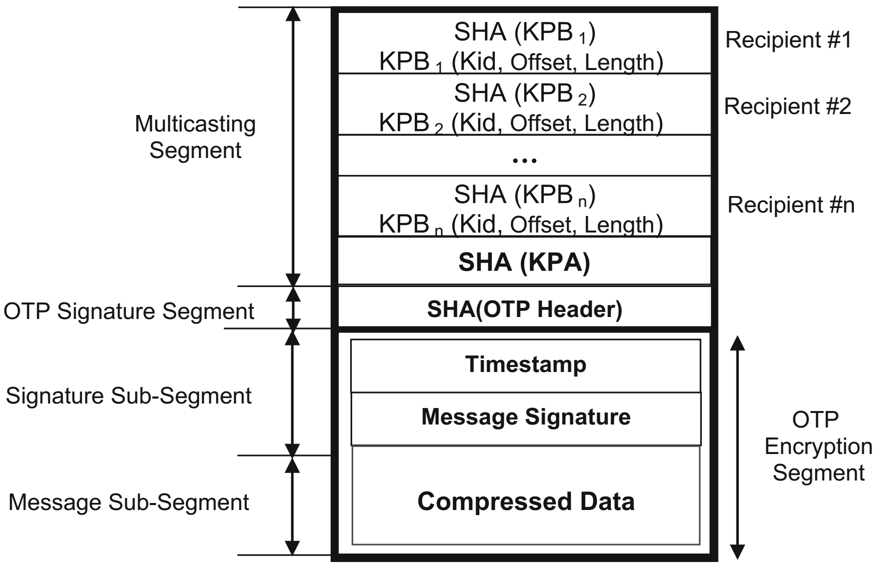

Fig. 2 The format of the transmitted message

- OTP Signature Segment: The signature segment includes: The hash code of the OTP Header, to identify the OTP to be used by the receiver to decrypt the message.

(ii) OTP Encryption Segment: It includes two sub-segments:

- Signature Sub-segment: It includes the timestamp and message signature.
- Message Sub-segment: It includes the timestamp (the time at which the encryption was made) and the compressed data to be stored or transmitted.

5. Theory of the Proposed Scheme

Hybrid cryptosystem is currently widely used, it combines the public-key and the secret-key cryptosystems, to gain the benefits of the public-key: the strength, unforgeable digital signature, and key management, and secret-key: the security and the performance. It is good and strong but still not ultimate. We are in need to a cryptosystem that achieve an ultimate security for sensitive applications. The security of cryptographic algorithms can be measured in many different ways, stressing different metrics [32–35]. The unicity distance can be applied to approach the security strength of the proposed scheme components.

The unicity distance of the overall system should be large enough to provide perfect secrecy. The individual components of the overall system are as shown in Fig. 3. The basic components of the proposed scheme, for which we can calculate the unicity distance, are the AES, and the OTP cipher. For the RSA algorithm, calculating the unicity distance is not worthy. The security of RSA depends on a

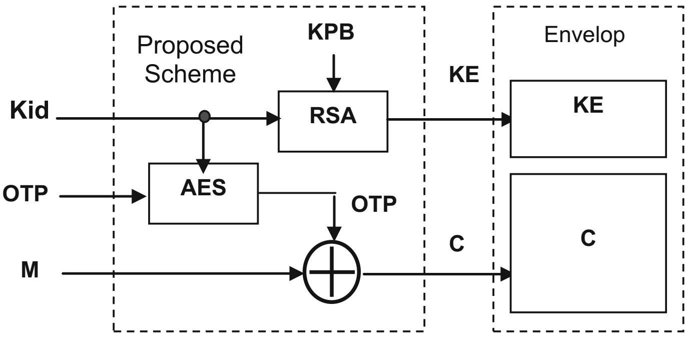

Fig. 3 Components of the proposed scheme

hard problem that is factoring of large composite numbers which is NP-hard problem.

Unicity Distance for the One-time Pad Cipher: The One-time Pad can be considered as a cipher with a period d equal to the message length. For s possible characters (All the alphabets, digits, and special characters i.e., s = 256 characters), we can calculate the unicity distance for the OTP cipher as follows:

$$U_{OTP} = H(K)/D = Log_2 s^d/D$$

where, H (K) is the entropy of the keys, d is the message length, and D is the redundancy of the language, we have:

$$\begin{aligned} U_{OTP} &= (Log_2 s/D)d \\ &= (Log_2 256)/(log_2 256 - 2(r))d \\ U_{OTP} &= 1.4\, d\, characters, \end{aligned}$$

where $r = 1.2$.

This means that, we need at least 1.4 times the length of the ciphered message.

Unicity Distance for the AES Cipher: The AES algorithm enciphers a 128-bit blocks (16 characters) using a 256-bit key. We can calculate the unicity distance of the AES algorithm as follows:

$$\begin{aligned} U_{AES} &= H(K)/D = (Log_2 2^{256}/(log_2 256 - 2.4)) \\ U_{AES} &= 45.714286\, characters \end{aligned}$$

This means that, the unicity of the AES is about three blocks.

6. The Proposed Scheme Parameters

The proposed scheme employs a four level of key hierarchy. This key hierarchy makes the scheme very difficult to break. These keys are One–time pad key, cryptographic random session key, RSA Private/Public key pairs and Pass phrase–based traditional key. The following parameters affected potentially on the secrecy and the performance of the proposed scheme.

In the proposed scheme, the OTP is a truly random sequence of bits. It is generated by a truly random bit generator and the generated random bits should pass the randomness tests. It is, then, stored in a compact CD. One CD will be exchanged physically between our extranet subscribers. Since our extranet represent a closed network environment, the number of subscribers will not be too much, that the above key management will be feasible. And the cost will be acceptable. The benefit against this cost is to provide a system with ultimate security. When a CD between the subscribers has been exhausted, it can be changed by a new one. The size of the compact CD is about 650 MB and expecting, under DVD Technology, to be of several GB's in the near future. This size seems to be reasonably enough for too many exchanged messages. The compact CD with this size can be practical, and physically exchanged securely between subscribers. As the size of the OTP increases, the cycle lifetime increases. The pointer that is mentioned in our scheme is in fact a dynamic pointer and consists of the following three parts:

(1) The starting offset on the sender CD from which the OTP ring is taken to encrypt the message by the sender.
(2) The length of the used OTP portion.
(3) The OTP Header, which is the fingerprint (SHA hashed value) for one Kbytes from the beginning of the used OTP ring. This can identify the correct OTP ring to decrypt the message correctly without any mistakes.

The AES Session key will be used only once per a message. The session key is a sequence of cryptographic random numbers generated using ANSI X9.17 [2] standard cryptographic random bit generator. It is generated each time a transmission is required. It is used to wash (encrypt) the OTP using the AES. The RSA algorithm is strong enough to protect the session key.

The security of RSA depends wholly on the problem of factoring large composite numbers. As the processing power capabilities increase, this becomes apparent. The increase in size of the RSA parameters becomes the sole solution to cover this attack. In our scheme, this attack is covered by implementing the RSA algorithm with variable key length parameters up to 8192 bits, which is seemed to be sufficient for future decade. Each participant entity should maintain his private key encrypted on a protected media like smart card or optical card token.

We need to generate the RSA keys, which are p, q, n, e, d, and u. The two main keys are p and q, from which the other keys can be derived. p and q must have certain criteria in order to achieve maximum security for the generated keys, hence ensuring the security of the encryption and decryption using these keys. These criteria are as follows:

(1) p and q must be prime, to ensure the proper formulation of the mathematical parameters which depending on them.
(2) p and q must be random numbers; in order to ensure the security of the keys, so that any attacker cannot guess the generated keys or know them if they were

generated starting from a given number, or using a fixed mathematical formula.

(3) p and q must not be too close together. These are because the public parameter key, n, is the product of p and q. If p and q were close together, an attacker can start searching for p or q from the square root of n, leading to fast finding of p or q.

Calculating the difference between p and q and finding if that difference is less than a given value does checking for closeness of p and q. That value is not a constant value but instead changes when p and q gets larger. The larger the values of p and q the larger that limit must be. So, the checking is done on the "relative difference" of the two numbers. The relative difference is the ratio of the value of the difference between the two numbers, p and q, and the value of the smaller of the two numbers (q). In our proposed system, the relative difference must be larger than 1/128 (0.0078). That is,

$$(p-q)/q > 1/128,\ (\delta = p-q),\ \delta/q > 1/12,\ \delta > q/128,\ log_2(\delta) > log_2(q) - 7.$$

This condition must be satisfied in order to ensure that the two numbers are not close together. If we have the two *RSA* parameters *p* and *q*, we can easily derive the other parameters *n, e, d*, and *u* using simple mathematical formulas as follows:

$$\Phi(n) = (p-1)(q-1),\ G(n) = GCD\,(p-1,\ q-1),\ F(n) = \Phi(n)/G(n)$$

Calculating the encryption parameter e: $GCD(e,\ \Phi(n)) = 1$. Calculating the decryption parameter *d and u and n as follows*: $e \cdot d \bmod F(n) = 1$, $p \cdot u \bmod q = 1$ and $N = p \cdot q.$

The best way to compute e is to use $F(n)$ because it tends to generate the smallest possible value for d that will match up with the two parameters e and n. This means that the decryption computations will be faster.

4 Results and Analysis of the Proposed Scheme

The strength of AES symmetric algorithm [2] or the strength of RSA asymmetric algorithm does not bound the security of the scheme. The strength of RSA is proved in this chapter. The RSA attack, the factoring problem, seems to be effective due to the increase in processing speeds in today's computing systems. Increasing the length of the RSA parameters can cover this attack. In our scheme, we implement the RSA algorithm with variable key length parameters that can deal with length up to 8192 bit [2].

AES algorithm is a 128-bit iterative block cipher with a 256-bit key and fourteen rounds. The security of AES algorithm depends on the use of three types of arithmetical operations on 32-bit words. One important principle in the design of

AES is to facilitate analysis of its features against cryptanalysis. AES is immune from differential cryptanalysis. In addition, no linear cryptanalytic attacks on AES have been reported and there is no known algebraic weakness in AES. The strength of AES is also guaranteed through the use of a session key only once per message. A 256-bit key seems to be reasonable enough.

If we assume, in the worst case, that the session key has been compromised, then we still have the OTP, which is exchanged, securely between our extranet subscribers. On the other hand, the vector sum modulo two operation employed is fast enough that it does not add any overhead or affect the performance of the scheme. As a conclusion, the OTP provides the security [36] of the scheme if AES or RSA keys have been compromised. On the other hand, if the OTP has been compromised the RSA and AES can guarantee the security of the scheme because we apply the washing process on the used OTP portion before the message encryption process.

The scheme employs the SHA to generate the message fingerprint. It provides 160-bit message digest. It is very hard to lie under the Birthday attack.

5 Conclusion

This chapter presents a new cryptosystem scheme for multiple secure and attack-resistant solutions for the applications of Internet and the future of IoT. Classification of existing security algorithms has been presented in this paper depending on their key bootstrapping approach to design and implement a secure communication system. A VPN can be built using tunneling technology, and include a set of subscribers representing the members of a closed system. Such environment is necessary for the sake of protection of the sensitive applications. We have demonstrated a new hybrid cryptosystem for IoT. It combines two standard cryptosystems, the RSA, and the AES, together with the one-time pad OTP. The security strength of the scheme has been measured and demonstrated. The one-time pad presents an ultimate security. The scheme has been implemented on a commercial PC, allowing the portability, maintainability, and availability for IoT applications.

References

1. Dorothy, E., Denning, R.: Purdue University, Cryptography and Data Security. Addison-Wesley Publishing Company (1983)
2. Schneier, B.: Applied Cryptography, Protocols, Algorithms, and Source Code in C, 2nd edn. Wiley (1996)
3. Atkins, D., Buis, P., Hare, C., Kelly, R., Nachenberg, C., Anthony Nelson, B., Phillips, P., Ritchey, T., Sheldon, T., Snyder, J.: Internet Security, Professional Reference. New Riders Publishing, Indianapolis (1997)
4. Charles, P.: Security in Computing. Prentice-Hall International Inc. (1989)

5. Brassard, G.: Lecture Notes in Computer Science, Modern Cryptology. In: Goos, G., Hartmanis, J. (eds.) (1988)
6. Goos, G., Hatmanis: Modern Cryptology, A Tutorial, Lecture Notes in Computer Science. Springer, Heidelberg (1988)
7. El Gammal, T.: A PUBLIC Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans. Inf. Theory **IT-31**(4) (1985)
8. Stalling, W.: Network and Internetwork Security. Printic Hall (1995)
9. Carl Ellison, M.: The Nature of a Usable PKI. Computer Networks (1999)
10. National Institute of Standards and Technology (NIST): The digital signature standard, proposal and discussion. Commun. ACM **35**(7), 36–54 (1994)
11. ElGendy, M.M., Dakroury, Y.H., El-Hennawy, M.E., Helail, F.A., Kouta, M.M.: A proposal for a new unconditionally secure hybrid cryptosystem. In: The Proceedings of the 35th Annual Conference on Statistics, Computer Science, and Operation Research, Part (111), Cairo, Egypt, November, pp. 115–129 (2000)
12. National Institute of Standards and Technology (NIST): FIPS publication 180. Secure Hash Stand. (SHS) (1993)
13. National Institute of Standards and Technology (NIST): Announcement of Weakness in the Secure Hash Standard (1994)
14. Robshaw, M.J.B.: MD2, MD4, MD5, SHA and other hash functions. Technical report TR-101, version 4.0, RSA Laboratories (1995)
15. Chabaud, A., Joux, A.: Differential Collisions in SHA-0, Centre d'Electronique de l'Armement CASSI/SCY/EC, F-35998 Rennes Armee, France, Advances in Cryptology—CRYPTO '98, Lecture Notes in Computer Science, vol. 1462, pp. 56–71 (1998)
16. National Institute of Standards and Technology (NIST): The digital signature standard, proposal and discussions. Commun. ACM **35**(7), 36–54 (1992)
17. Roman, Rodrigo, Zhou, Jianying, Lopez, Javier: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**, 2266–2279 (2013)
18. Chatterjee, T.: Symmetric key Cryptosystem using combined Cryptographic algorithms—Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm, 978-1-4673-0125-1 IEEE, p. 1179 (2011)
19. Baek, J.: Compact identity-based encryption without strong symmetric cipher. In: ASIACCS'11, March 22–24, 2011, Hong Kong, China, pp. 61–70. ACM 978-1-4503-0564-8/11/03
20. Acharya, B.: image encryption using index based chaotic sequence, M sequence and gold sequence. In: ICCCS11, Rourkela, Odisha, India, pp. 541–544, ACM 978-1-4503-0464-1/11/02, 12–14 Feb 2011
21. Kusters, R.: Computational soundness for key exchange protocols with symmetric encryption. In: CCS'09, Chicago, Illinois, USA, pp. 91–100, ACM 978-1-60558-352-5/09/11, 9–13 Nov 2009
22. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC'09, Bethesda, Maryland, USA, pp. 169–178, ACM 978-1-60558-506-2/09/05, May 31–June 2 2009
23. Ateniese, G.: Provably-secure time-bound hierarchical key assignment schemes. In: CCS'06, Alexandria, Virginia, USA, pp. 288–297, ACM 1-59593-518-5/06/0010, October 30–November 3, 2006
24. Nishanth, R.B., Ramakrishnan, B., Selvi, M.: Improved Signcryption Algorithm for Information Security in Networks. Int. J. Comput. Netw. Appl. (IJCNA) **2**(3) (2015)
25. Alagl, Y.S., El-Alfy, E.S.M.: SwiftEnc, hybrid cryptosystem with hash-based dynamic key encryption. In: The 7th International Conference on Information Technology, ICIT (2015)
26. Malhotra, R.: A hybrid geometric cryptography approach to enhance information security. J. Netw. Commun. Emerg. Technol. (JNCET) **3**(1) (2015)
27. Saeed, Q., Al-Khalidi, Y.: E-Commerce Business Using Hybrid Combination Based on New Symmetric Key and RSA Algorithm, vol. 20, no. 1, pp. 59–71. National Chengchi University and Airiti Press Inc. Securing (2014)
28. Nguyen, K.T., Laurent, M., Oualha, N.: Survey on secure communication protocols for the internet of things. Ad Hoc Netw. **32**, 17–31 (2015)

29. Cabarcas, D., Demirel, D., Göpfert, F., Lancrenon, J., Wunderer, T.: An unconditionally hiding and long-term binding post-quantum commitment scheme. Cryptol. ePrint Arch. Rep. **628** (2015)
30. Sinha, S.K., Shrivastava, M., Pandey, K.K.: A new way of design and implementation of hybrid encryption to protect confidential information from malicious attack in network. Int. J. Comput. Appl. **80**(3), 0975–8887 (2013)
31. Kalra, S., Sood, S.K.: Secure authentication scheme for IoT and cloud servers. Pervasive Mobile Comput. **24**, 210–223 (2015)
32. Shannon, C.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
33. Beker, H.: Cipher Systems: The Protection of Communications. Wiley (1983). ISBN 0-471-89192-4
34. Menezes, A., et al.: Handook of Applied Cryptography. CRC Press, New York (1997)
35. Schneier, B.: Crypto-gram (1998)
36. Moreira, N., Molina, E., Lázaro, J., Jacob, E., Astarloa, A.: Cyber-security in substation automation systems. Renew. Sustain. Energy Rev. **54**, 1552–1562 (2016)