International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 6, December 2018, pp. 5443~5448
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp5443-5448

Secure Privacy Implications for Clients and End-users through Key Assortment Crypto Techniques Implicated Algorithm

D. Ramesh, B. Rama
Department of Computer Science, Kakatiya University, India

Article Info

Article history:

Received Feb 23, 2018
Revised Jul 9, 2018
Accepted Jul 30, 2018

Keyword:

Key-Logging Facility (KLF)
Pure-Ciphertext (PCT)
Pure-Plaintext (PPT)
Single Mode Encryption (SME)

ABSTRACT

The main role of key assortment crypto techniques will helpful to provide the security to the sensitive data and play the key role for business developments. Some of the problems are rising when the scheme will sustain the possession control to present the latest set of technical and business concerns. Some of the complex challenges are waiting for the optimistic solutions. The challenges are: In the planned storage confidentiality implicated outline, the stipulation of encryption framework for the data which is conserve the self tunning to execute major key constratints by concerining their files which is imposed plaintext belonging, the owners of the privacy-data preserve the seclusion power over their own information to formulate assured wide-ranging service operations and the owners of data are facing the complexity to organize their possess data which is accessible-mode in cloud servers, concerned inner services: topology architecture type of implicated data with their operations, associated secrecy-privacy-secrecy dynamic replicas for make use of the databased security within their range of format and secretarial services with their encrypted data execution control. To overcome theses in convinces this paper is proposing the technical ideals through the algorithmic methodology along the graphical flow-based architecture. This paper is proposing the key assortment crypto techniques implicated algorithm for clients and end-users to reduce the above mention complex difficulties; it describes the primary encryption implicated techniques and various levels of cryptographic algorithms with their implications along with extensions of cloud implicated data security and digital forensics implicated appliances which is implicated with enhanced various hash functions.

Corresponding Author:

D. Ramesh,
Department of Computer Science,
Kakatiya University,
Warangal, Telangana, India.
Email: rameshd525@gmail.com

1. INTRODUCTION

The cloud computing is a centralized distributed network implicated framework with the provision of an assortment of federal cloud reliable services to the clients along with their end users [1] with concern of mutual agreements between the cloud enterprises and end user clients by implicating the major services of cloud environmental flexible data storage, retrieval, security, privacy and in-time execution and high securable data delivery with help of provided consent client environmental implicated key assortment implicated crypto techniques to evade and confine the unconstitutional accessibility [2], [3]. Owners of data store their data in cloud which therefore need to be secured. By storing data in encrypted form, one can maintain the confidentiality and privacy of data in cloud. In CC the various cryptographic implicated approaches are formulated to address the subject of secrecy and privacy of authenticated-user generated.

The authors Prasanna and Akki did detail descriptive investigation on cloud computing implicated privacy concern, security issues, challenges and cryptographic implicated algorithms [4]. Cryptography is the knowledge of writing in top secret code and is an ancient art [5]. In the cloud computing environment, the maintenance of authorization and provision of control over the data is a distinct prerequisite over and above assess and to authenticate the primary security of the cloud service providers implicated environment [6]. The unfortunate information revelation will cause affects the data possessor status, economic reputation, and impact their regulatory and legal compliance needs [7]. The encryption techniques are the best and sophisticated data protection mechanism to derive the methods to protect the treasured data, the protection layers formed in the forms of secret keys to represent the privacy implicated data [8].

The Encryption implicated Integrity (EbI) is implicated on the technologies and progression of leading the cryptographic security depended services [9], [10]. Encryption is a crucial and important data along with their appliance implicated protection technique and the encryption keys should be accurately supervised and protected. The appearance of cloud implicated services will liberation of effective security implicated services, and also it implicated the encryption implicated capabilities which are utilized to secure the privacy data especially in the cloud implicated environment, and also it provide the chances and to enable the all kinds of organizations to easily protect their sensitive data through the internal key-logging based facility (KLbF) [11], [12]. When cryptography is used to protect treasured data, the risk is transferred from the content to the keys and the protection of cryptographic keying material becomes paramount once the encryption has been designed in a systematic way.

The crucial concern positioned in the way of cloud depended adoption implicated boundary is the requisite for trading to retain the possession and also to control of their own data while it is in progression and accumulate at cloud implicated service providers (CbSP) [6]. In present days, many organizations are willing to move towards to the cloud implicated environment it may capitulate the information implicated security (IbS) enhancement where the CbSP stick on to the third-party dependent frameworks. In cryptography mechanism, the un-encrypted data (UED), referred to as pure-plaintext (PPT). The PPT can be transmitted and encrypted into pure-ciphertext (PCT), which will in turn (usually) be decrypted into usable plaintext environment [13].

2. DETERMINED EXERTIONS AND SECURE CONCERNS

The main role of key assortment crypto techniques will helpful to provide the security to the sensitive data and play the key role for business developments [14]. Some of the problems are rising when the scheme will sustain the possession control to present the latest set of technical and business concerns. Some of the complex challenges are waiting for the optimistic solutions. The challenges are:

a. The cloud implicated service provider will not isolate the primary functionality of data-owners self control mechanism from their own privacy data.
b. In the planned storage confidentiality implicated outline, the stipulation of encryption framework for the data which is conserve the self tunning to execute major key constratints by concerining their files which is imposed plaintext belonging
c. The owners of the privacy-data preserve the seclusion power over their own information to formulate assured wide-ranging service operations and the owners of data are facing the complexity to organize their possess data which is accessible-mode in cloud servers, concerned inner services: topology architecture type of implicated data with their operations, associated secrecy-privacy-secrecy dynamic replicas for make use of the databased security within their range of format and secretarial services with their encrypted data execution control.

To overcome theses in convinces this paper is proposing the algorithmic methodology along the graphical flow based framework and it recommending the key assortment crypto techniques implicated algorithm for clients and end-users to reduce the above mention complex difficulties; it describes the primary encryption implicated techniques and various levels of cryptographic algorithms with their implications along with extensions of cloud implicated data security and digital forensics implicated Appliances which is implicated with enhanced various hash functions.

3. CRYPTOGRAPHIC AND HASH IMPLICATED ALGORITHMIC IMPLICATIONS

The encryption techniques are the best and sophisticated data protection mechanism to derive the methods to protect the treasured data, the protection layers formed in the forms of secret keys to represent the privacy implicated data. The cryptographic implicated algorithms are classified into various ways and it will be characterized by the number of key-points are deployed for generating the encryption and decryption mechanisms and by their implicated Appliance sequences. The hashing implicated algorithmic (HbA)

principles will act like as significant responsibility in terms of securing the systems by certify the reliability of the trusted implicated data communication. The HbA translates the variable-depended-length text field into a fixed-size-string and it primarily used in a security implicated systems with the two concerns [15] which are

a. Single mode hashing method: the derived the hash implicated output; it is complex to reverse the hashing implicated functions to generate the original message.
b. Non-collision implicated output method: for a hashing implicated algorithm, it is computationally infeasible to find any two messages which are the same hash output. Here the hash is treated as message digest or digital fingerprint by considering these two properties.

The individuals are producing a small-hash-output from a bulky-document and use the digital fingerprint of the document as the hash implicated output. This type of digital fingerprint will be used to make sure that the data has not been interfering while it is transmission mode when is passing through the low-secure communication media. In addition, from the digital fingerprint, it is not possible to disclose the content of the original message. The message-digest-algorithm 5 (MD5) and Secure Hash-Algorithm-1 (SHA-1) are the widely used and implemented cryptographic hash implicated algorithms. These two types of hashing algorithms have been measured as the one-way and powerfully collision-free hashing algorithms. 128-bit output has been formed by MD5 and 160-bit output has been formed by SHA-1. Normally, the SHA-1 is measured as high-securable implicated on its larger size, but computationally it's more expensive than MD5. The SHA-1 is the favoured hashing implicated algorithm for implicating the VPN deployment mechanism. With the hardware and software implementation in today's networks, the performance difference is usually not a concern [16].

4. KEY ASSORTMENT CRYPTO TECHNIQUESIMPLICATED ALGORITHMIC SEQUENCES

As per shown in the flow chart Figure.1 and the algorithm, the methodology has been implicated in two levels of execution such as end-user implicated signatures and Appliance implicated segments. The Appliance implicated segments can be processed and implicated from the clients or end-users signatures.

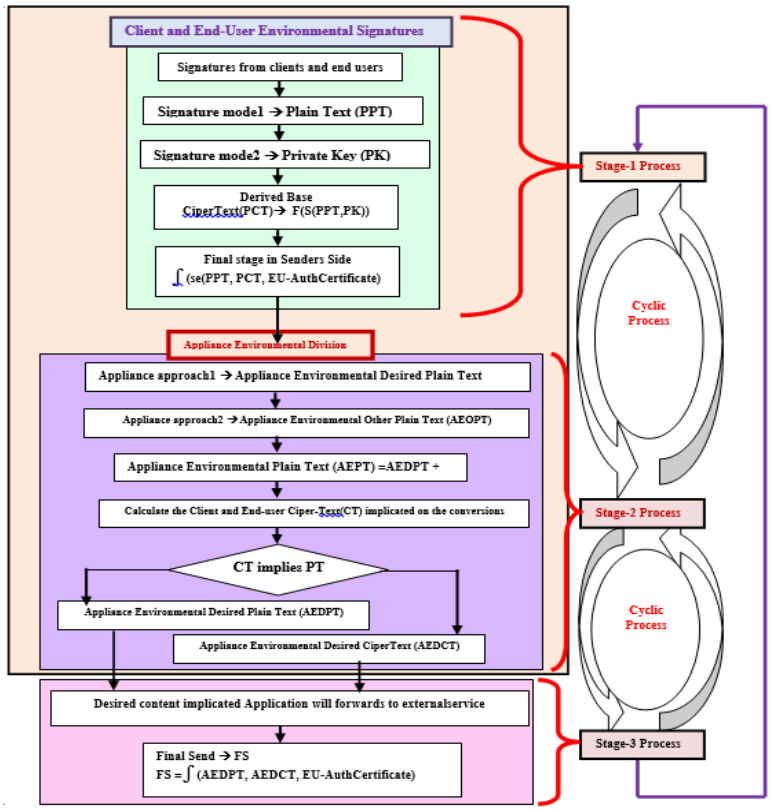

Figure 1. Execution flow chart of client and end-user environmental signatures and appliance environmental division

4.1. Client and End-User Environmental Signatures

The first level of execution composes the initial authenticated sequences about the end-user implicated signatures through plain text (PPT) of signature mode1, private key (PK) of signature mode2 along with the derived base class environment as shown in the Figure1. The derived base class can be composing the ciper text (PCT) by making the single set with two various elements of signatures such as PPT and PK.

F(S(PPT,PK)) ← Derived Base (PCT)

The final stage can be prepared from the sender's side environment with help of the function generation with the elements of PPT, PCT, EU-AuthCertificate values.

∫ (se(PPT, PCT, EU-Auth-Certificate)

Finally, the generated final stage of operations will be pushed into the second level execution mode of Appliance implicated segments for further up gradations such as update or modify the existing data or enhancement of new data along with the existing data.

4.2. Appliance Environmental Division

The second level of execution composes Appliance implicated segments by deriving the two stages of Appliances modes such as Appliance mode1 and Appliance mode2 as shown in the Figure 1. Here the first level of Appliance mode can holds the Appliance implicated desired plain text (AbDPT) and the second level of Appliance mode can holds Appliance implicated plain text (AbOPT) which is belongs to other plain text. This second level of Appliance mode is the enhanced version of Appliance mode1; it contains the new added or updated data of the particular specified Appliance of the particular enterprise. These two various levels of Appliance modes can be combined together to update the final version of the genuine data in cloud.

The user need to add its final version of the data into the cloud server in his specified storage location without giving or advertising by its own existing or modified network architecture along with its own resources like as current active users, internal private accessibility keys and VPN environments. Generally, the cloud environment can restrict the end users to store their enhanced version of data to their existing data when they changed or modified their internal recourses which are not included when they get the resources services from cloud initially. This algorithmic techniques can transmits enhanced data to cloud storages to patch it with its own existing data with sending any private information about the client or end users. This filtering mechanism can be process through the computing the end-users cipertext (CT) implicated on their conversions. The CT implies the PT for deriving the AbDPT and AbOPT. Finally, the derived enhanced Appliance implicated contents will be forwarded to external service and added to the cloud implicated server by FS implicated sequence as shown in Figure 1.

FS = ∫ (AbDPT, AbDCT, EU-AuthCertificate)

4.3. Algorithm

Statement 0: End-User implicated signatures
Gathering the signatures from the end-users / data owners
Statement 1: Gathering the mode1 implicated signature
Plain Text (PPT) ← Signature mode1
Statement 2: Gathering the mode2 implicated signature
Private Key (PK) ← Signature mode2
Statement 3: Compose the derived base class
F(S(PPT, PK)) ← PCT
Statement 4: Senders side preparation to push the data for up-gradation
∫ (se (PPT, PCT, EU-AuthCertificate)
Statement 5: Appliance Environmental Division: Appliance approach1
Appliance approach1→ Appliance implicated Desired Plain Text (AbDPT)
Statement 6: Appliance Environmental Division: Appliance approach2
Appliance approach2→ Appliance implicated Other Plain Text (AbOPT)
Statement 7: Appliance Environmental Plain Text (AEPT) will be generated by combining the Appliance Environmental Desired Plain Text and Appliance implicated Other Plain Text
Appliance Environmental Plain Text (AEPT) =AbDPT + AbOPT

Statement 8: Comparison will be needed without advertising the end-users updated private environment for deriving the Appliance implicated Desired Plain Text and Appliance Environmental Desired CiperText

IF CT implies PT

THEN Appliance Environmental Desired Plain Text (AbDPT)

THEN Appliance Environmental Desired CiperText (AbDCT)

Statement 9: Desired content implicated Appliance will forwards to externalservice

Statement 10: Finally stage of storage the enhanced data

Final Send → FS

FS = ∫ (AbDPT, AbDCT, EU-AuthCertificate)

And the services will verify this message as while the user had generated or sent it directly. The above implicational sequences will well work implicated on the type of hash algorithm has been implemented to squeeze the PPT also organism of homomorphic generation. Amongst them the homomorphic implicated and searchable encryption methods are largely fashionable where one can perform computation and search on PCT exclusive of revealing the PPT [3].

5. CONCLUSION

The main role of key assortment crypto techniques will helpful to provide the security to the sensitive data and play the key role for business developments. The main problem will be raised when the system will maintain the ownership control and to present the latest set of technical and business concerns. This paper is proposing the key assortment crypto techniques implicated algorithm for clients and end-users to reduce the above mention complex difficulties; it describes the primary encryption implicated techniques and various levels of cryptographic algorithms with their implications along with extensions of cloud implicated data security and digital forensics implicated Appliances which is implicated with enhanced various hash functions.

ACKNOWLEDGEMENTS

I would like to thankful to my supervisor, colleagues and friends.

REFERENCES

[1] Ericsson, 2015, "Encryption Performance Improvements of the Paillier Cryptosystem", available at: https://eprint.iacr.org/2015/864.pdf

[2] Mell, Peter and Tim Grace, "Draft NIST Working Definition of Cloud Computing", http://csrc.nist.gov/groups/SNS/clouddcomputing/cloud -def-v15.doc, on August 2009.

[3] Prasanna B T, C B Akki, "A Comparative Study of Homomorphic and Searchable Encryption Schemes for Cloud Computing".

[4] Prasanna B.T, C.B. Akki, "A Survey on Homomorphic and Searchable Encryption Security Algorithms for Cloud Computing". *Communicated to Journal of Interconnection Networks*, April 2014.

[5] Gary C. Kessler , "An Overview of Cryptography, Handbook on Local Area Networks", *Auerbach*, Sept. 1998.

[6] Vaultive Encryption in Use Platform, Taking Control of Cloud Data: A Realistic Approach to Encryption of Cloud Data in Use", *Vaultive Inc. 489 5th Ave, 31st Fl.New York, NY* 10017. www.vaultive.com

[7] Gigaom Research, 2014, "Data Privacy and Security in the Post-Snowden Era", available at: http://www.verneglobal.com/sites/default/files/gigaom_research-data_privacy_and_security.pdf

[8] Cloud Security Alliance, "SecaaS Implementation Guidance, Category 8: Encryption", September 2012, http://www.cloudsecurityalliance.org,

[9] Gutman, P., Naccache, D., & Palmer, C.C. (2005, May/June). "When Hashes Collide". *IEEE Security & Privacy*, 3(3), 68-71.

[10] PERC, 2015, "Secure Real-time Transport Protocol (SRTP) for Cloud Services", available at: https://tools.ietf.org/html/draft-mattsson-perc-srtp-cloud

[11] Cryptography in an all Encrypted world charting the future of innovation, volume 92 | #10 December 22, 2015, Ericsson Technology Review Cryptography in an all Encrypted world Security in the post-snowd.

[12] Fraunhofer Institute for Secure Information Technology. (2012, March). On the Security of Cloud Storage Services. Retrieved from http://www.sit.fraunhofer.de/de/cloudstudy.html

[13] AceWG, 2015, Object Security of CoAP (OSCOAP), available at: https://tools.ietf.org/html/draft-selander-ace-object-security

[14] European Network and Information Security Agency (ENISA). (2009). Cloud Computing benefits, risks, and recommendations for information security. Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[15] AccessData. (2006, April). MD5 Collisions: The Effect on Computer Forensics. AccessData White Paper.
[16] Qiang Huang and Jazib Frahim, SSL VPN Technology, Network World | Oct 22, 2008 http://www.networkworld.com/article/2268575/lan-wan/chapter-2--ssl-vpn-technology.html

BIOGRAPHIES OF AUTHORS

D Ramesh completed M.Tech (Computer Science) From School of IT,JNTU Hyderabad and pursuing PhD in the department of Computer Science, Kakatiya University, Warangal. Present working as Assistant Professor in Computer Science, Department of Computer Science, University Campus College, KakatiyaUniversitysince eightyears. Area of interest is Cloud Computing, cryptography Network Security. Published papers in IEEE InternationalConferences and International Journals.

Dr B.RAMA received her Ph.D. Degree in Computer Science from Padmavati Mahila Visvavidyalayam, Thirupathi, India in the year of 2009. She is working as Assistant Professor in Computer Science at Department of Computer Science, Kakatiya University. Her area of interest is Artificial Intelligence and Data Mining. She is the author or co-author of various scientific, technical papers in Scopus, IEEE, Springer International, National Journals and Conferences.