IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

# Public Key Cryptography on Symmetric Encryption Based on Session Time Key Verification for Securing the Data in Cloud

**Mrs. D. Annalakshmi[1], Dr. C. Jayanthi[2], Mrs. A. Rukmani[3]**

Research Scholar, PG & Research Department of Computer Science, Government Arts College (Auto), Karur, Tamil Nadu, India[1,3]

Assistant Professor, PG & Research Department of Computer Science,Government Arts College (Auto), Karur, Tamil Nadu, India[2]

**ABSTRACT:** Day to day development of information sharing in network needs advancement in securitybecause various attacks, data theft, false injection occurs on transmission. By concerning the security improvement, **Crypto Policy Standards (CPS)** becomes the most important part to take overthe data protection using optimized encryption schemes. Due to the nonstandard protocols in cryptographic encryption, data be insecurebecause of key failures, defect made decryptionoccurs leads data losses. To resolve this problem, to implement a **SymmetricStandard based public key CryptographicSystem (SSCS)** to improve the security reaches. In Addition, Crypto Policy Protocolsare optimized with **Advanced Encryption Standard (AES)** using bootstrappingencryption standards to protect the data. Thispublic key cryptographic system manages the symmetric single key authentication without pair verification to protect the data who wants to access using this key. Over the network transmission the request session is verified with symmetric key to acknowledge the request access from data ownerpermission. The key is bootstrapped with random access encrypted protocols. The **Multi party authentication (MPA)** verifies the service request by owner authentication after providing the key to access the data. This improves the higher security which they concerns data leakages, improvedauthentication, key validation and time consumption. The network data is primary aspect of the network providers and service providers. Therefore during the information exchange the cryptographic techniques are utilized for securing the information during various communications. At the same time the traditional cryptographic techniques are well known and the attackers are known about the solution. Therefore new type of cryptographic technique is required which upgrade the secured and complexity of information cipher. Most of the RSA, DES implementation of Public Key Encryption to improve the security on wireless sensor networks with authenticationLeakages.

**KEYWORDS:** CPS, MPA, AES, Cryptographic, Public key, Encryption, Security, Description, Bootstrap method.

## I. INTRODUCTION

The network data is primary aspect of the network and service providers. Therefore during the data exchange the cryptographic techniques are utilized for securing the data during various communications. Alternatively the traditional cryptographic techniques are well known and the attackers are known about the solution. Therefore this kind of cryptographic technique is required which improves the safe and complexity of data cipher. Most of the RSA, DES implementation of Public Key Encryption to improve the security on wireless sensor networks with authentication leakages.

### Public Key Cryptography

Each user has two keys: one encryption key that he makes public and another one is decryption key that keeps secretly, it shouldbe computationally infeasible to determine the decryption key given only the encryption key and the cryptographic algorithm. Each user generates a two set of keys to be used for encryption and decryption. Each user apply any one of the above keys in a public register and the other key is kept in private.

Basically the key generation can be divided into few categories of algorithms which are Discrete Logarithm, Integer Factorization,Coding Theory, Elliptic Curve, Lattices, DigitalSignature and Hybrid. Each scheme

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

optimized with crypto policy needs such as to ensure the security of the scheme as well as to save space and time during data communication. The modified optimization single signing factorschemes were proposed to increase the security aswell as to increase the speed of encryption anddecryption time. In order to overcome theproblem, several schemes had been introducedthat are capable of encrypting one bit at a time.

**Symmetric Key Encryption Standard**

The most technique of symmetric-keysystem is the Data Encryption Standard (DES). DES uses 56-bit keys. The Key are shortest to be easily randomized single key by modern hardware and it is recommended that DES should not to be used. Three DES uses 128 bits key length. Symmetric key algorithms are sometimes calledas secret key algorithms. This single unique key is used for encryption and decryption. Public-key encryption avoids this problem because the publickey can be distributed in a non-secure way, and the private key is never transmitted.

## II. LITERATURE SURVEY

- Author / Title / Techniques used / Limitations

- C, Shoushan luo, and Hongmin GAO / (2018) / " Key Escrow Protocol based on a Tripartite Authenticated Key Agreement and Threshold Cryptography". Based on the elliptic curve cryptosystem and the advanced encryption standard. / They also make it easier for malicious users to discuss and plot illegalactivities such as key leakages.

- Author / Title / Techniques used / Limitations

- Hisham N. Almajed, Ahmad. S. Almogren / (2019) / "SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography", IEEE. / Trusted and proofed scheme that offers authenticated encryption. The main issues with asymmetriccryptography is the need lack of storage.

- Author / Title / Techniques used / Limitations

- Manisha Malik, Maitreyee Dutta / (2019) / "A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in theInternet of Things", IEEE / key bootstrappingprotocols based on public-key cryptography. The lack of secure links exposes data exchanged by devices to theft and attacks, with hackers already showing a keen interest in this area.

- Author / Title / Techniques used / Limitations

- M. G. G. Ganesh / (2018) / "Secure method for text encryption using elliptic curve cryptography". / Elliptic curve cryptography is a methodology to public key cryptography based on algebraic structure. These techniques eliminate the expensive process of mapping authentication whereas it pop- ups an essential need to share the common lookup chart amongst the sender and the receiver.

- Author / Title / Techniques used / Limitations

- H. Hong and Z. Sun, / (2018) / "Achieving secure data access control and efficient key updating in mobile multimedia sensor networks", IJMIR. Encryption scheme to guarantee the secure data sharing in MMSN. Due to its better performance in monitoring the target environment, MMSN has already been applied to many fields and scenarios.

- Author / Title / Techniques used / Limitations

- Leihong Zhang, Xiao Yuan / (2019) / "Multiple Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography", IEEE. Multiple- Image Encryption method based on Hadamard basis patterns and RSA public key cryptography. / The problem of low quality of traditional random illumination patterns and increases the security of the system.

-

## III. PROBLEM IDENTIFICATION FACTORS

Communication Network security was not carefully carried out through key policies, since only some symmetric encryption based protocols are used at base end. The problem of security concerning by the use of public key cryptography as single, by ensuring the authenticity of the user request doesn't concentrate the owners policy. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a insecure way because of intent attacks. Public-key encryption holds data encryption problem becausethe public key can be distributed in a non-secure way, and the private key is never transmitted to made probable reverse decryption.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

The security of the Single signing encryption scheme relies on the quadratic residual problem. Nevertheless, one most important drawback of this scheme was required large number of random bits and produce large amounts of cipher text. Due to this problem consumes data leakages, security less provisions in key authentication false verifiable access and time complexity.

## IV. OBJECTIVE OF THE RESEARCH

To implement secure public key cryptography on symmetric encryption (SPKC- SE) based on session time key verification for securing the data in cloud data. The proposed system integrates the exponential max confidence random encryption to improve the data security. To design a Session Time based Integrity Key Authentication (ST-IKA) data with additional key verification session request to improve the public key generation using the service level auditing protocol. To design the short-term variation detection or verifying the integrity of, which they determined for the Dynamic Auditing Service (DAS) to improve the security. To project a Multiparty Bootstrapping Authentication (MBA) for Improving Network security based on block security. We proposed a new concept of block homomorphic equality test algorithm and with valid authentication schemas to increase the integrity as well security to reduce key leakages with time consumption.

## V.PROPOSED SOLUTION AND IMPLEMENTATION

The public-key encryption is based on access key functions, which are easy to compute, but hard to reverse without additional information. The session key based encryption optimized with RSA be use the public-key algorithm, in which the hard problem is finding the prime factors of a composite number. In Public Key Cryptographic system, generally in a key pair, the public key and the private key, the public key is permitted to access to the public and the private key is kept at a safe place. In PUBLIC KEY CRYPTOGRAPHY system, public or private key pairs can be easily generated for encryption and decryption.

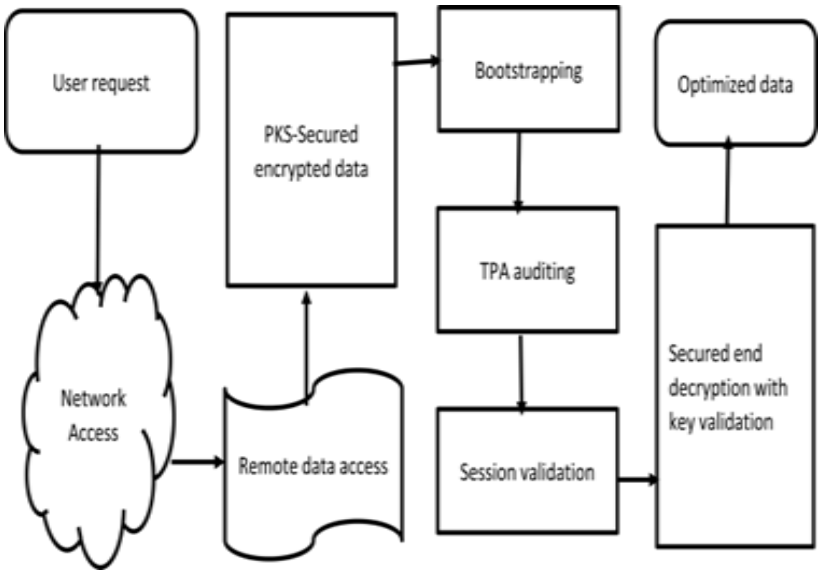


**Fig. 1: Architecture diagram to improve the security**

### Public Key Crypto Policy

To encrypt a message with the public key of an entity, public key encryption is utilized where only the entity with the corresponding private key is capable of decrypting the cipher text. Cipher text generated in Digital signatures with the private can be decrypted by anyone who has the public key. This verification determines that the sender had access to the private key and therefore is likely to be the person associated with the public key.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

**Multi-Objective Crypto System**

The security strength in a PUBLIC KEY CRYPTOGRAPHY system improves the signing authentication form both a properly generated private key from its public key. For brute-force attacks, the length of private is most important. The AES is one of the optimized public-key crypto systems, which is based on the practical difficulty of factoring the product of two large prime numbers. Multi objective considers the Session, authentication of key logs, data audit ability using PA produce more security on single sign verification factor to improve the security.

**Symmetric Session Key Based Encryption**

The session time maintains the data with additional key verification and session request to improve the public key generation using the service level auditing protocol. The third party integrates the session key embedded in the data stored in a single storage. This system improves the on-time secured verification using the public key cryptography security system with the right factor of using the dynamic auditing protocol. If the public key is large enough, the prime numberscan feasibly decode the message in only the known way. The optimized algorithm forencryption however it is commonly used to pass encrypted shared keys for symmetric keycryptography.

**Multiparty Bootstrapping Authentication**

The key problem of achieving fully homomorphic encryption is how to reduce the increasing noise during the cipher text evaluation. Bootstrapping procedure can refresh cipher text with large error. So, the resulting cipher text has potentially smaller error in ciphers and allows being continuous homomorphism evaluation. Based on the block homomorphic equality testalgorithm, a faster bootstrapping procedure with smaller bootstrapping keys are determined. Both Key and block ciphers validate key authentication to produce high performance of our bootstrapping algorithm. A faster bootstrapping procedure basedon the block homomorphic equality test algorithm.

## VI. RESULT ANALYSIS

The above defined mechanism improves the performance in Integrity, Availability, Authentication, Non- repudiation, Confidentiality and Access control. This is achieved by private- public into singular key model as the user is restricted both at sender and receiver end which is restricted in other models.

**Integrity -** The reliable and ensured data is protected from unauthorized changes.

**Availability -** Timely and uninterrupted access of the system is protected by its availability.

**Confidentiality -** The unauthorized accessing and monitoring of data objects and resources are protected by its confidentiality.

**Access control -** It is a restriction of accessing resources in access management which defines theprocess.

**Non-repudiation** - Ensuring that communication of accepting the authenticity of their signature in adocument.

## VII.CONCLUSION

The conclusion begins that the security using public key cryptographic security are optimized with symmetric session key using multi-party Bootstrapping authentication. The best security performance using the session time key verification for securing the data in Network communication. The method selects the encryption to be used as similar way service acceptance for decryption whether the valid request at in session expired time. Based on the service session completeness measure themethod allows or deny the user request. The dataencryption and public auditing are enforced in service level which increases the performance of session time public auditing as provide best authentication. The proposed method improvesthe performance in public verification, throughput and reduces the time complexity as well.

## REFERENCES

[ 1 ] M. G. G. Ganesh, "Secure Method for Text Encryption using Elliptic Curve Cryptography", International Journal of Advance Scientific Research and Engineering Trends Int. J., vol. 3, no. 11, pp. 11_15, 2018.

[ 2 ] Hisham N. Almajed, Ahmad S. Almogren, " SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography", December 5,2019, volume 7, pp: 175865-
175878.

[ 3 ] Manisha Malik, Maitreyee Dutta, and Jorge Granjal, "A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things", March 13, 2019. pp: 27443- 27464.

[ 4 ] C, Shoushan Luo, and Hongmin GAO, " KeyEscrow Protocol based on a TripartiteAuthenticated Key Agreement

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

and ThresholdCryptography", October 24, 2019. Pp: 149080-
149096.

[ 5 ] Z. Wang, Z. Ma, S. Luo, and H. Gao, "Enhanced Instant Message Security and Privacy Protection Scheme for mobile social network systems", IEEE Access, vol. 6, pp. 13706_13715, 2018.

[ 6 ] H. Hong and Z. Sun, "Achieving Secure Data Access Control and Efficient Key updating in mobile Multimedia Sensor Networks", Multimedia Tools Appl., vol. 77, no. 4, pp. 4477_4490, 2018.

[ 7 ] Leihong Zhang, Xiao Yuan, Kaimin Wang, and Dawei Zhang, " Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography", Volume 11, Number 4,
August 2019, pp-1- 15.

[ 8 ] T. N. Tan, H. Lee, "A Delay - Efficient Ring -LWE Cryptography Architecture for Biometric Security", in Proc. IEEE Int. Symp. Circuits Syst.,Baltimore, MD, USA, May 2017, pp. 2210 – 2213.

[ 9 ] Shreya Dey, Ashraf Hossain, " Session- KeyEstablishment and Authentication in a Smart Home Network using Public Key Cryptography",IEEE-2019, pp:1-4.

[ 10 ] F. Albalas, M. Al-Soud, O. Almomani, and A. Almomani, "Security-Aware CoapApplication layer protocol for the Internet OfThings using Elliptic Curve Cryptography", Power (mw), The International Arab Journal of Information Technology, vol. 15, no. 3A, p. 151, 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com



Scan to save the contact details