International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (17-27), Month: January - April 2015, Available at: www.noveltyjournals.com

Software Quality Assurance in Network Security Using Cryptographic Techniques

Ayesha Manzoor[1], Sidra Shabbir[2], Ms. Mehreen Sirshar[3]

[1,2,3] Fatima Jinnah Women University, the Mall Rawalpindi, Pakistan

***Abstract*: The use of the network communication has imposed serious threats to the security of assets over the network. Network security is getting more prone to active and passive attacks which may result in serious consequences to data integrity, confidentiality and availability. Various cryptographic techniques have been proposed in the past few years to combat with the concerned problem by ensuring quality but in order to have a fully secured network; a framework of new cryptosystem was needed. This paper discusses certain cryptographic techniques which have shown far better improvement in the network security with enhanced quality assurance. The scope of this research paper is to cover the security pitfalls in the current systems and their possible solutions based on the new cryptosystems. The development of new cryptosystem framework has paved a new way to the widespread network communications with enhanced quality in network security.**

I. INTRODUCTION

The advancements in the technology with ease of access has made us live in a computer world now, all our daily works and communications are shifted to computers. The reduction in manual efforts has resulted in a computer medium everywhere. Computer use has enormously increased since the last decade with growing use of internet and transmissions over the network. To ensure quality in the network security we need to have a strong framework of security services. Because computers using internet are vulnerable to attacks like viruses, worms, Trojans and hackers of systems. People are more interested in exploiting privacy of others and intend to manipulate their data thus making the network insecure for the users. So there is need to develop methods and algorithms that can make the network reliable for transmission of assets by making it more secure.

Network security is the process of ensuring secures communication over the internet and secure transmission of data among different computers. Different techniques are to make secure communication over the internet. One of the technologies discussed in this research is cryptography. Cryptography is basically secret writing. It involves adding secure information to the original message by encrypting it, this message is decrypted at the receiver side using some decryption algorithm. Network security provides authenticated access, confidentiality and maintains integrity of data.

II. SURVEY PAPERS SUMMARIES

1. Visual Cryptography

Cryptography ensuring encryption mechanism sometimes may not provide ultimate security leading to serious threats to security goals. To address large scale vulnerabilities we need Secret Sharing scheme (SSS) to protect information content items like secret images. Since image sharing is a popular mean of transmitting information so various secret sharing schemes are developed to achieve security. In existing systems the receiver only gets the share and stack to decode the secret image and no verification is done to avoid cheating while in SS scheme the receiver receives the verification image in addition to the secret image and no cheating can be done. This scheme can be applied on black and white as well as the colored images. The image is divided into n number of shares through random number generator and uses less mathematics as compare to current scheme of cryptography on colored photos but the drawback is that the number of loops keep on increasing and iteration are stuck lead to complexity. So there is need of scheme that proposes same solution with less number of iterations.

2. Quantum Cryptography: An Emerging Technology in Network Security

Mostly digital systems depend on the currently used cryptosystems for integrity and confidentiality of their traffic across the network. However there are some limitations in current cryptosystem related to most important parameters like key refresh rate and key expansion ratio etc. Therefore many organizations have insecurities about their assets. To cater with these weaknesses new advancements have led to the development of quantum cryptography based on quantum mechanism. The unique character of this technique is detection of third party between communicating users by the way of quantum key distribution (QKD) technique thus providing secure network. However there are some challenges in implementation of this technique like development of advance hardware for longer transmission of quantum key. So we can infer that limitations in current cryptography will pave ways towards continued advancements of quantum cryptography leading to valuable contribution to network security.

3. Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET

Cryptographic techniques can be used to make network secure however attackers can misuse by making use of flaws in the scheme's design of web applications framework ASP.NET. Some highly practical and efficient attacks lead to tracing of secret key by decryption of the code hence providing access to private assets. Some abusing component present in the framework like ASP.NET for application development provides the necessary information about decrypting the code. It is not possible even for the developers to implement secure cryptography in such framework. Scripting languages like ruby, python, PHP provide cryptographic libraries in connection to Open SSL which is a stronger tool providing secure low-level libraries. Unauthenticated encryption is harmful as it leads to random, serious attacks to the real system. Therefore the cryptographic API needs to involve the authentication mechanism and also their integration for providing secure cryptography.

4. Security in Wireless sensor network security using Cryptographic technique

The advancements in the wireless security networks have made them widely used in different applications. Therefore it’s the need of the hour to make them secure by fulfilling the security goals like confidentiality, authentication, integrity and availability. But there are a lot many limitations in wireless sensor networks like fewer resources, capability of process and less storage capacity. One widely used method for security is by means of an appropriate cryptographic technique. RSA and Elliptic curve cryptography are two widely used public key algorithms. ECC is better than RSA because it lessens the time of computation, uses low memory and amount of data to be transmitted.

However a new advancement in the form of Multivariate quadratic scheme has shown better result by providing more security.

5. Survey on the Applications of cryptography

Cryptography is secret writing technique that ensures protection of private data against unauthorized access by making use of mathematics for securing data. It has been emerged as a secure mean of data transmission with fulfillment of security goals like data integrity and confidentiality. Different types of cryptography include Public key cryptography used in secure data transmission, key Escrow cryptography in monitoring the communications, translucent cryptography in fractional observance of data and symmetric key cryptography in file transmission over network. Cryptography has wide range of applications which involve certificates and authentications. Apart from that one time pad technique is used to keep secrets for secure transmissions. Hence cryptographic techniques can be used for making network secure for data transmissions.

6. Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method

Wireless sensor networks consist of system of sensors and actuators working in coordination with environment. Due to their sensitivity they need to be made secure because they are more prone to attacks. Certain security challenges like wireless mechanism, evenly distributed nodes in the environment with fewer resources have made WSN less secure thus threatening data integrity, confidentiality and availability. Therefore public key cryptographic algorithms RSA and ECC are employed and their energy analysis is counter checked. Analysis on the result of Sun SPOT test shows that RSA consumes more energy or battery power as compared to ECC and under low key bit size both have same security level. However ECC is far better in its processing capabilities and computing power against RSA

7. Secured Communication through Fibonacci Numbers and Unicode Symbols

Cryptography refer to secret writing and is yet been considered a secure way of transmitting message between two people without involvement of any third body. It can be implemented in number of traditionally used ways but there are some drawbacks with each. Cryptography using public key, secret key or through hash function have certain weaknesses. Public key cryptography is significantly slow and subjected to frequent attacks. One method is replacement of character in plain text with character relevant to generated Fibonacci number and cipher text is translated into Unicode symbols. At the decrypting end extraction algorithm gets back the pain text from Unicode symbols. So evolution of cryptography from traditional substitution to Unicode code has made it a better mean of data hiding, authenticating and preventing unauthorized access. Using this way helps in transmitting secret information through secure channel in a simple, different and easy way.

8. Secure Key Exchange through Elgamal Cryptosystem in ADHOC Networks

ADHOC Networks share a common radio channel for the exchange of key but there are certain special characteristics that make ADHOC networks more prone to attack like their dynamic-natured topology, data loss and link breakage, limited range of transmission and bandwidth. A large number of nodes make it difficult to achieve a fully secured channel for communication. This problem can be solved by another technique of cryptography based on exchanging key through ELGAMAL cryptosystem which is an asymmetric key algorithm that makes use of node from formulation of binary trees. Nodes can be added using insertion mechanism and connection is established and can be deleted using deletion mechanism. Hence security is achieved with reduction in issues related to rekeying and prevents overheads in key distribution.

9. Cryptographic techniques in mobile ad-hoc networks

Mobile ADHOC network is a wireless self-organized network of mobile nodes. To make it more secure and also self-manageable cryptographic techniques can be used. The scheme uses new nodes that can join and others can leave the network at any time. The addition of new nodes enhances the functionality and work as initial node by obtaining its secret key in order to authenticate itself. The node can be any wireless device such as PDA, cell phone or laptop. These nodes manage whole life of the MANET in a decentralized process. The main advantage of this process is that network is secure without involvement of any third trusted party. So we have a scheme that proposes full dynamism and decentralization in the Mobile ad-hoc network thus making it secure and effective.

10. Secret Key Cryptography Using Graphics Cards

Cryptographic protocols are not widely used because of their poor performance of algorithm and their impact on whole system however another approach involves simultaneous processing of large amount of data through Graphic Processing Units (GPU). GPU is a better scheme to reduce some load from a processing main CPU and proves to be very beneficial for the system’s performance as a whole. The encryption and decryption mechanism used in the GPU with potential applications in image processing can help in joining connection of data segments with key at a time however when there is a dedicated CPU, this processing cannot be done simultaneously. Currently demand based on the GPU processing power is increasing the needs of users. Hence a secret key connection with private data segment helps in achieving a secure platform for transmitting sensitive information among communicating users.

11. Enhancement of Network Security Techniques using Quantum Cryptography

This paper provides comparison of classical cryptography and Quantum cryptography. This paper proposed “**Secured Quantum cryptography algorithm**”. This algorithm uses concepts of both classical and quantum cryptography. Some other algorithms discussed are Shore’s Algorithm and Grover’s Algorithm etc. It safely sends data. Using **shore’s**

algorithm it offers efficient, fast and secure systems that are not easy to break. It provides support to large size of bits, so there are minimum chances of making random numbers for this algorithm. Quantum physics gives decoherence and hardware unavailability. This technique is applied in ultra secure voting, secure communication with space, smart power grid and quantum internet.

12. A New Modular Multiplication Method in Public Key Cryptosystem

This paper proposed new algorithm "**modular multiplication"** used for many public key cryptosystems. Two computation methods are describes, first is to look for the residue from the residue with modulus and residue with modulus and second is that how prime numbers are factorized to give prime factors. The **Chinese theorem** can be applied to find remainder. This algorithm maximizes the speed for exponential based systems. It can break into infinite numbers of prime factors, hence it decreases the complexity. It helps to improve the speed of signal processing systems. This technique can be applied in RSA Cryptosystems, digital signature schemes, EI Gamal cryptosystems, elliptical curve systems and Robin systems.

13. Performance Based Comparison Study of RSA and Elliptic Curve Cryptography

This paper provides the comparison between RSA algorithm and elliptic curve cryptography. **RSA algorithm** is simple, more secure; use digital signature method. **Elliptic curve cryptography** is public key cryptography. It has fast encryption speed, less memory and has small key size. The basic addition operation is very expensive, so it cannot recognize sub-exponential attacks. RSA algorithm knows sub-exponential attacks. So it develops key pair more efficiently. To select right key is hard to find in RSA. RSA algorithm has slow encryption speed. RSA is more trustworthy as compared to ECC. RSA algorithm is used widely to secure internet, banking, and credit card processing.ECC algorithm is used in cryptographic message systems.

14. Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET

This paper provides comparison between symmetric and asymmetric cryptographic algorithms by using parameters like speed, block size and key size. **VANET** is used for wireless networks communication. Symmetric Encryption Method use a share a key and Asymmetric Encryption Method uses two different keys for sender and receiver. Symmetric Encryption Method is easy and fast. It uses less computer resources, small key size and needs separate secure channel to exchange key. Asymmetric Encryption Method key encryption method uses simple arrangement of symmetric keys. It is slow, needs large size of key, and its security is provided by hard mathematical laws.RSA is not suitable for encryption of long messages. Elliptic Curve Cryptography requires less memory, small power for computation, and small size key. Large size messages require long computing time so cannot be encrypted using VANET.VANET used for avoiding dangerous crashes, warning the driver about weather, road, traffic, and driving rules.

15. Review and Analysis of Cryptography Techniques

This review paper discusses the methods of cryptography on the basis of their respective research papers in journals. Rivest Shamir and Adelman **algorithm** fails in Wireless sensor network because it is complex. But it is can easily be changed and platform independent. **Digital signature algorithm** uses "**Hash method**" that is used to send small size data and does not disclose data. **Elliptic key cryptography** used for small size of key and uses mathematical concepts. ECC is used for smart card applications because it is efficient. **Dieffie-Hellman algorithm** exchanges the unspecified key between sender and recipient. In short ECC algorithm is efficient than RSA because of its small key size. Dieffie-Hellman algorithm is applied in all techniques used by internet. Mobile nodes use RSA because they are open to righteous attacks due to their broadcast category.

16. Network Security Using Cryptographic Techniques

This paper manage the test and produce results by using crypto Tools as simulator. Network security is a significant component of information security. **Cryptographic techniques** are used to yield network security by encryption/decryption of data. It gives data that is protected from harm over wireless networks. Network security using cryptography uses a lot of algorithms to give unharmed conveyance of data. It protects network and hide the personal operations accomplish by users. Symmetric cryptographic systems and Asymmetric cryptographic systems are two types of cryptosystems. A**symmetric cryptosystems** have problems of sharing key. It disowns Digital signatures. **Symmetric cryptosystems** uses a public key. It personalized the digital signatures. Cryptography techniques are applied in information security for safe conveyance of data over the network.

17. Review on Encryption Ciphers of Cryptography in Network Security

This paper describes many block ciphers, stream ciphers and hashing algorithm. Three **goals of network security** achieved using cryptographic techniques. Plaintext is transformed to make cipher text. **Stream ciphers** are efficient as compared to block. **Block ciphers** are more expensive because they are applicable on large size of data. Stream ciphers are hard to develop. Stream ciphers can modify the data but block ciphers do not modify the contents of data. Stream ciphers are needs high execution speed but have less hardware complexity. Block Ciphers are applicable in cipher text stealing. Stream ciphers are applicable in hardware because they are simple and efficient.

18. Applied Cryptography and Network Security

This paper describes the Security Analysis of an Open Car Immobilizer Protocol Stack. Openness is key criteria for security algorithms and protocols. This paper describes the example of car immobilizer applications. This process of security systems is not always secure. Most probably when the algorithm is disclosed then security threat arises through various channels. A car immobilizer uses a key fob to run a car. If this key is not applied then car's engine Control unit does not work properly.

An open security protocol stack is used. It implements user command interface. It issued number of commands by reader to the key. Authentication is done in one way or two way.AES block cipher is applicable in implementation of many commands by reader and fob.

19. Network Security: Attacks, Tools and Techniques

This paper elaborates the major attacks in network security and offers possible solutions. Network security makes sure that data is disclosed to the person who claims it. **Network security attacks** harms the useful information placed on the network, moreover it slow down the processing speed and generates harmful executable files that spread on the network to destroy the data. It damages the disk of our systems. We can overcome all these security threats by scanning the systems on regular basis. We should use latest versions of software and application programs for our systems. We should use unique and secure passwords. We should carefully logout from any website. **Security technologies** should be applied in online network processing to secure the processing over network.

20. Encryption Using Different Techniques: A Review

This paper explains different cryptographic techniques. Public key is shared at both sides in symmetric cryptography whereas different key are used in asymmetric cryptography. RSA is used for getting factorial of big prime numbers. Digital signatures introduce mathematics in cryptography. DSA is used in electronic mail. RSA algorithm is not applicable in WSN due to their complexity. Dieffie Hellman algorithm used for exchanging many keys. **Digital signature** maintains the originality of data. These all cryptographic techniques are applicable in ATM cards, computer passwords and electronic commerce. We concluded that all the cryptographic techniques discussed above are applicable in the real time encryption.

III. ANALYSIS

Table 1 shows the quality parameter definition. Table 2 show the results of analysis of evaluation parameters defined in evaluation criteria in Table 1. This research paper is the survey of 20 research papers and their evaluation is done using 15 evaluation parameters. Table 2 shows that customizability regarding Cryptography in Network security is not considered in any of the research table.

[3] R.Y.Rao et al, 2013, S.V.Gunti et al, 2014, [9] M.Panda, 2014, [11] G.A.V.Rama et al, 2013, [12] R.Sinha et al, 2013, [13] N.Kaur et al, 2011, [14] F.Bao, 2012, [15] M.Alimohammadi et al, 2014, [16] S.Kaushik et al, 2012, [17] G.Gupta et al, 2012, [18] S.Ghansela, 2013 and [20] N.Jirwan et al, 2013 address the **reliability** attribute of the system.

They refer to attachment of new nodes at any time in the existing networks, RSA and ECC methods are discussed for public key encryption thus ensuring secure key exchange through elagmal Cryptosystem. But to select right key is hard to find in RSA. RSA algorithm has slow encryption speed. RSA is more trustworthy as compared to ECC.

[1] V.Daza et al, 2007, [3] R.Y.Rao et al, 2013, [4] A.Kaur, 2013, [5] M.S. Sharbaf, 2011 addressed the **efficiency** attribute of the cryptographic techniques proposed by them. Quantum cryptography is efficient in terms of identifying presence of third party in communication. Key Escrow cryptography, Stream ciphers and block ciphers, translucent cryptography, symmetric key cryptography techniques have been proposed to increase the efficiency in promoting network security. Digital signature maintains the originality of data. . Elliptic key cryptography used for small size of key and uses mathematical concepts. ECC is used for smart card applications because it is efficient. But the basic addition operation is very expensive with ECC, so it cannot recognize sub-exponential attacks

[10] T.Duong et al, 2011, [11] G.A.V.Rama et al, 2013, [14] F.Bao, 2012, [15] M.Alimohammadi et al, 2014, [20] N.Jirwan et al, 2013 addressed the **reusability** attribute of the system. The concept of graphic cards in the system with reusability ideas promotes security. Secured communication using Fibonacci numbers and Unicode symbols helps to achieve the secured means of transmission over the network. But it is **not efficient** method, as it involves computing complexity.

[1] V.Daza et al, 2007, [2] A.J.Raphael et al, 2012, [3] R.Y.Rao et al, 2013, [4] A.Kaur, 2013, [7] S.V.Gunti et al, 2014 discussed the availability attribute of the system. The nodes attachment technique at any time helps promote availability of the network through secured public key cryptographic channel.

[4] A.Kaur, [6] S.Goyal, [8] D.L.Cook et al, [9] M.Panda and [13] N.Kaur et al, 2011 addressed the **confidentiality attribute** of the system. The visual cryptographic technique ensures the confidentiality of visual data. The image is divided into n number of shares through random number generator and uses less mathematics as compare to current scheme of cryptography on colored photos but the drawback is that the number of loops keep on increasing and iteration are stuck lead to **complexity**.

Cost effective parameter is discussed in the research papers [13] N.Kaur et al. It discusses RSA algorithm that is simple, more secure. Because of its simple computation mechanism it is cost effective. Another algorithm is discussed in the paper that was Elliptic curve cryptography that is fast, need less memory and has small key size. The basic addition operations in ECC are very **expensive** and cannot recognize sub-exponential attacks. RSA is better than ECC is term of cost.

[15] M. Alimohammadi et al and [16] S.Kaushiket al, 2012 discusses **portability** parameter of software quality assurance. The paper describes Rivest Shamir and Adleman algorithm that fails in Wireless sensor network because it is complex. But it is can easily be changed and **platform independent**. Digital signature algorithm uses “Hash method” that is used to send small size data and does not disclose data.

[12] R.Sinha et al, 2013 discussed **performance** attribute of quality assurance and proposed new algorithm “**modular multiplication”** used for many public key cryptosystems. This algorithm maximizes the speed for exponential based systems. It can break into infinite numbers of prime factors, hence it decreases the complexity. It helps to improve the speed of signal processing systems.

[15] M.Alimohammadi et al, 2014 discussed **ease of use** attribute. The paper explained Dieffie-Hellman algorithm that exchanges the unspecified key between sender and recipient. But it is not an efficient method to transfer unspecified keys between sender and receivers.

[17] G.Gupta et al, 2012 discussed reliability, ease of use, **efficiency, portability, integrity and functionality** attributes for ensuring software quality in network security using cryptography. It discussed two ways of processing the cipher text stream cipher and blocks cipher and then compares them in terms of the above mentioned attributes. **Stream ciphers** are efficient as compared to block. **Block ciphers** are more expensive because they are applicable on large size of data.

Stream ciphers are hard to develop. Stream ciphers can modify the data but block ciphers do not modify the contents of data. Stream ciphers are needs high execution speed but have less hardware **complexit**y. Block Ciphers are applicable in cipher text stealing. Stream ciphers are applicable in hardware because they are simple and **efficient**.

[19] S.SHAKTI, 2013 describes following parameters named as: ease of use, functionality, efficiency, extendibility, confidentiality, verification, validation, cost effectiveness, and performance. It described network security attacks and then recommends tools, techniques and algorithms to make secure the network. **Network security attacks** harms the useful information placed on the network, moreover it slow down the processing speed and generates harmful executable files that spread on the network to destroy the data. It damages the disk of our systems. We should use unique and secure passwords. We should carefully logout from any website. **Security technologies** should be applied in online network processing to secure the processing over network.

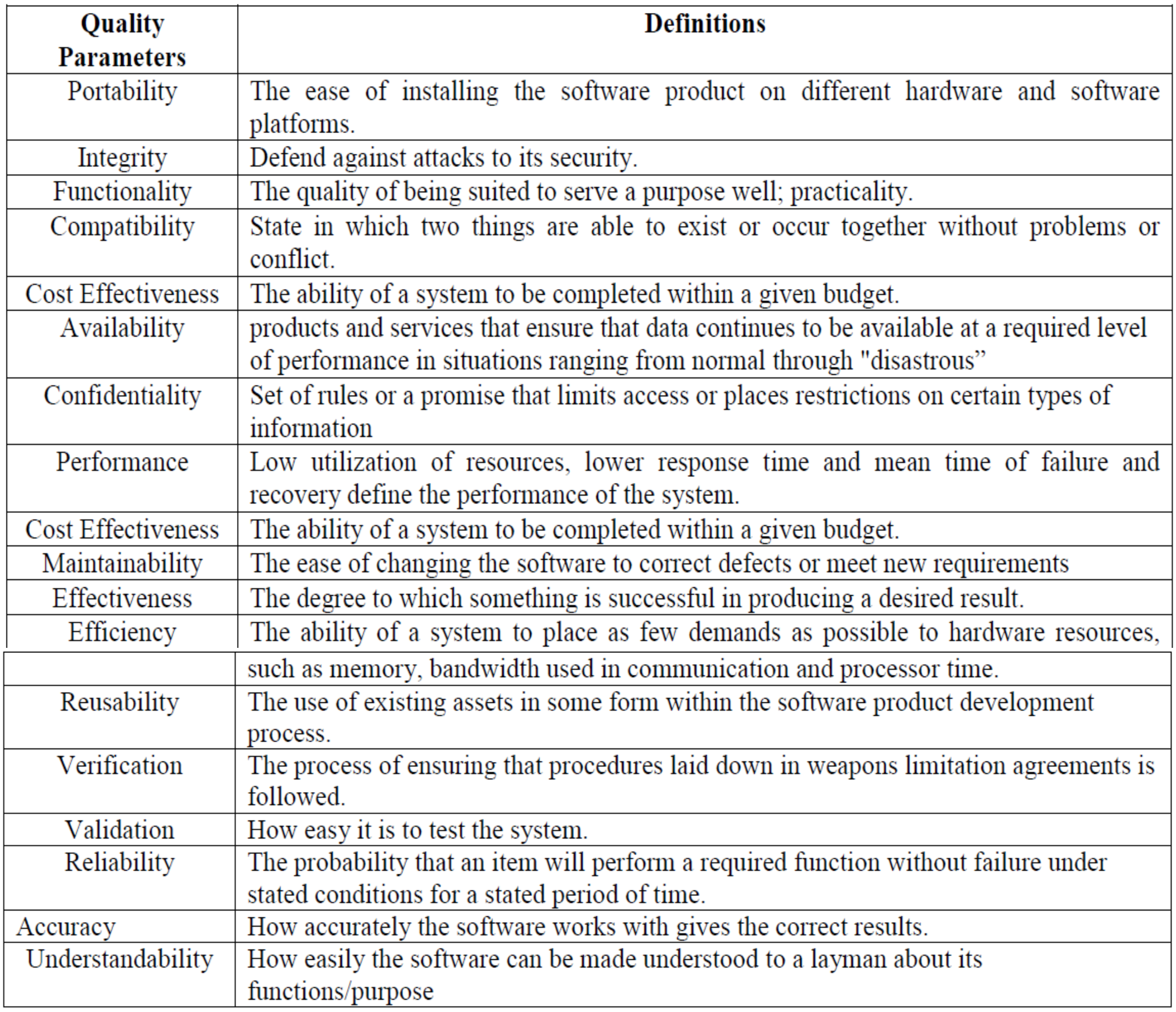
Possible Values

1. Yes

This parameter is explicitly mentioned in the Research paper.

2. No

Table-1



Quality Parameters	Definitions
Portability	The ease of installing the software product on different hardware and software platforms.
Integrity	Defend against attacks to its security.
Functionality	The quality of being suited to serve a purpose well; practicality.
Compatibility	State in which two things are able to exist or occur together without problems or conflict.
Cost Effectiveness	The ability of a system to be completed within a given budget.
Availability	products and services that ensure that data continues to be available at a required level of performance in situations ranging from normal through "disastrous”
Confidentiality	Set of rules or a promise that limits access or places restrictions on certain types of information
Performance	Low utilization of resources, lower response time and mean time of failure and recovery define the performance of the system.
Cost Effectiveness	The ability of a system to be completed within a given budget.
Maintainability	The ease of changing the software to correct defects or meet new requirements
Effectiveness	The degree to which something is successful in producing a desired result.
Efficiency	The ability of a system to place as few demands as possible to hardware resources, such as memory, bandwidth used in communication and processor time.
Reusability	The use of existing assets in some form within the software product development process.
Verification	The process of ensuring that procedures laid down in weapons limitation agreements is followed.
Validation	How easy it is to test the system.
Reliability	The probability that an item will perform a required function without failure under stated conditions for a stated period of time.
Accuracy	How accurately the software works with gives the correct results.
Understandability	How easily the software can be made understood to a layman about its functions/purpose

Table-2

S #	Authors	Reliability	Integrity	Reusability	Maintainability	Ease of Use	Efficiency	Portability	Functionality	Extendibility
1	V.Daza et al, 2007	No	yes	No	yes	No	Yes	No	No	Yes
2	A. J.Raphael et al, 2012	No	Yes	No	No	Yes	No	No	No	No
3	R.Y.Rao et al, 2013	Yes	Yes	No	No	No	Yes	No	yes	Yes
4	A.Kaur, 2013	No	Yes	No	Yes	No	Yes	No	No	Yes
5	M.S. Sharbaf , 2011	Yes	Yes	No	Yes	No	Yes	No	No	No
6	S.Goyal, 2014	No	Yes	No	No	No	Yes	No	No	No
7	S.V.Gunti et al, 2014	Yes	No	No	No	No	No	No	No	No
8	D.L.Cook et al , 2014	No	Yes	No	No	No	Yes	No	Yes	No
9	M.Panda, 2014	Yes	Yes	No	No	Yes	Yes	No	No	Yes
10	T.Duong et al, 2011	No	Yes	Yes	Yes	No	Yes	No	Yes	No
11	G.A.V. Rama et al, 2013	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No
12	R.Sinha et al, 2013	Yes	No	No	Yes	Yes	Yes	No	Yes	No
13	N.Kaur et al, 2011	Yes	Yes	No	No	Yes	Yes	No	Yes	No
14	F.Bao, 2012	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
15	M.Alimohammadi et al, 2014	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16	S.Kaushiket al, 2012	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes
17	G.Gupta et al, 2012	Yes	Yes	No	No	Yes	Yes	No	Yes	No
18	S.Ghansela, 2013	Yes	No	No	Yes	No	No	No	Yes	No
19	S.SHAKTI, 2013	No	No	No	No	Yes	Yes	No	Yes	Yes
20	N.Jirwan et al, 2013	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table-3

S #	Authors	Confidentiality	Availability	Verification	Validation	Cost effective	Accuracy	Understandability	performance
1	V.Daza et al, 2007	No	Yes	Yes	No	Yes	No	No	No
2	A.J.Raphael et al, 2012	Yes	Yes	No	No	No	No	No	No
3	R.Y.Rao et al, 2013	Yes	Yes	Yes	Yes	No	No	No	No
4	A.Kaur, 2013	Yes	Yes	Yes	No	Yes	No	Yes	Yes
5	M.S. Sharbaf , 2011	Yes	No	No	No	No	Yes	No	Yes
6	S.Goyal, 2014	Yes	No	Yes	No	yes	No	No	Yes
7	S.V.Gunti et al, 2014	No	Yes	No	No	No	No	No	No
8	D.L.Cook et al , 2014	No	No	Yes	No	Yes	No	No	Yes
9	M.Panda, 2014	Yes	Yes	Yes	No	Yes	No	No	Yes
10	T.Duong et al, 2011	No	No	No	Yes	Yes	No	No	Yes
11	G.A.V. Rama et al, 2013	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
12	R.Sinha et al, 2013	No	Yes	Yes	yes	No	Yes	Yes	Yes
13	N.Kaur et al, 2011	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
14	F.Bao, 2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
15	M.Alimohammadi et al, 2014	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16	S.Kaushiket al, 2012	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
17	G.Gupta et al, 2012	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
18	S.Ghansela, 2013	Yes	Yes	Yes	Yes	No	No	Yes	No
19	S.SHAKTI, 2013	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
20	N.Jirwan et al, 2013	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

IV. CONCLUSION

The research paper has discussed certain cryptographic techniques which have been proposed in the last few years in order to improve security across the network. Network communications are getting more secure now but still there are few limitations of these techniques. Greater number of iterations in secret sharing scheme has made it complex to be implemented, the high level mathematics in the Elgamal and Fibonacci number with Unicode symbol technique has made it little harder to code, use of RSA leads to slower speed with greater computational time thus decreasing efficiency, rekeying issues in the quantum key distribution such as need of increased key refresh rate has limited its scope similarly public key cryptography is slow and more subjected to cryptanalytic attacks so there is need of strong technique with high level of confusion and diffusion in order to ensure quality in network security. Recently a new advancement in the form of Multivariate quadratic scheme is introduced which has shown better results by reducing complexity in terms of implementation and has increased confusion and diffusion for secure transmissions across the network. It is the need of hour to improve quality of network security in order to ensure a fully secured transmission of assets over the network.

REFERENCES

[1] M. Sirshar and Dr.F.Arif "Evaluation of Quality assurance Factors in Agile Methodologies", February-2012

[2] http://searchstorage.techtarget.com/definition/data-availability

[3] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[4] http://kedar.nitty-witty.com/blog/software-quality-attributes-parameters explained#sthash.lqvAV1DO.dpuf

[5] http://kedar.nitty-witty.com/blog/software-quality-attributes-parameters explained#sthash.lqvAV1DO.dpuf

[6] V.Daza, J.Herranz, P.Morillo and C.Ra`fols," Cryptographic techniques for mobile ad-hoc networks",26 August 2007.

[7] J.Raphaeland Dr. V.Sundaram.," Secured Communication through Fibonacci Numbers and Unicode Symbols", International Journal of Scientific & Engineering Research ,Volume 3, Issue 4, April-2012.

[8] R.Y.Rao, R Swetha and P.Ramanjaneyulu," SECURE VISUAL CRYPTOGRAPHY", International Journal of Scientific & Engineering Research, Volume 4, Issue3, March-2013.

[9] A.Kaur,"Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method", International Journal of Scientific & Engineering Research,Volume 4, Issue 5, May-2013.

[10] M.S. Sharbaf," Quantum Cryptography: An Emerging Technology in Network Security", 978-1-4577-1376-7/11/$26.00 ©2011 IEEE.

[11] S.Goyal,"A Survey on the Applications of Cryptography", International Journal of Science and Technology, Volume 1 No. 3, March, 2012.

[12] S.V.Gunti", Secure Key Exchange Through Elgamal Cryptosystem In Adhoc Networks", International Journal of Scientific & Engineering Research ,Volume 5, Issue 4, April-2014

[13] D.L.Cook, J.Ioannidis and A.D.Keromytis," Secret Key Cryptography Using Graphics Cards", January 14, 2004.

[14] M.Panda," Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER), Volume-03, Issue-01, pp-50-56, 2014.

[15] T.Duong and J.Rizzo," Cryptography in theWeb: The Case of Cryptographic Design Flaws in ASP.NET", 2011 IEEE Symposium on Security and Privacy.

[16] G.A.V.Rama,C.Rao, P.V.Lakshmi and N.R.Shankar," A New Modular Multiplication Method in Public Key Cryptosystem", International Journal of Network Security, Vol.15, No.1, PP.23-27, Jan. 2013.

[17] R.Sinha, H.k. Srivastava and S.Gupta," Performance Based Comparison Study of RSA and Elliptic Curve Cryptography", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[18] N.Kaur et al, “Enhancement of Network Security Techniques using Quantum Cryptography”, International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 5 May 2011.

[19] F.Bao and P.Samarati,J.Zhou,”Applied Cryptography and Network Security”, 10th International Conference, ACNS 2012 Singapore, June 26-29, 2012.

[20] M. Alimohammadi and A. A. Pouyan,” Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET”, International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014.

[21] S.Kaushik and A.Singhal,”December 2012.Network Security Using Cryptographic Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12.

[22] G.Gupta and R.Chawla ,” Network Security: Attacks, Tools and Techniques” ,International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 2, Issue 7, July 2012.

[23] S.Ghansela ,“Network Security: Attacks, Tools and Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 3, Issue 6, June 2013.

[24] S.SHAKTI, ”Encryption Using Different Techniques”, International Journal in Multidisciplinary and Academic Research (SSIJMAR),vol. 2, No. 1, January-February-2013.

[25] N.Jirwan, A.Singh and Dr.S.Vijay,”Review and Analysis of Cryptography Techniques”, International Journal of Scientific & Engineering Research, Volume 4, Issue3, March-2013.