International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2064125

The Literature Review on The Role and Significance of Cryptography for Network Security in Current Scenario

Praful Kr. Ranjay[1], Prof. Dr. Ramdip Prasad[2], Arif Md. Sattar[3]*
[1]Department of Computer Science, Magadh University, Bodh Gaya, India
[2]Department of Mathematics, Danapur College, Patna, India
[3]Department of Computer Science, Anugrah Memorial College, Gaya, India

ABSTRACT

As the internet has gotten more integrated into our daily lives and has grown exponentially over the last several decades, data security has become a major issue for everybody connected to the internet. Data security ensures that only the intended recipients have access to our information and prohibits any data modification or manipulation. Various techniques and approaches have been developed to reach this level of security. Cryptography is described as a set of techniques for encrypting data using specified algorithms that render the data unreadable to the naked eye unless decoded using procedures predefined by the sender. We cover some of the most recent research in the fields of cryptography and network security in this article. The security vulnerabilities of existing as well as upcoming technologies in the field of Computer Networks are discussed in these research articles. We bundle the articles together based on their content and categorise the research subjects based on their implementation throughout the seven layers of the well-known OSI reference model. In the interest of brevity, the main purpose for each research study is outlined, and the proposed solution is stated simply.

Keywords : Network Security, Data Security, Cryptography, Internet, OSI Model

I. INTRODUCTION

Cryptography is a method of ensuring message confidentiality. In Greek, the phrase has a special meaning: "hidden writing." Nowadays, however, individuals and organisations' privacy is protected by high-level cryptography, which ensures that information delivered is secure and only the authorised receiver has access to it. Cryptography is a traditional method that is continuously being explored, with historical roots. Examples date back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as additional evidence from ancient Greece and Rome, such as secret writings and the renowned Caesar cypher.

Hundreds of millions of people use cryptography on a regular basis to protect data and information, while the majority are unaware of it. Cryptographic systems, in addition to being incredibly valuable, are also extremely brittle, as a single programming or specification error can compromise them.

We live in an information age, which necessitates the storage of data on every element of our life. This information may be regarded of as an asset, and like any other asset, it must be protected against attacks. Information must be hidden from unauthorised access (confidentiality), protected from unauthorised change (integrity), and accessible only to an authorised entrance when it is needed to be secure (availability). As a result, the three most critical

security goals are confidentiality, integrity, and availability.

Computers have unquestionably grown omnipresent in today's world, and as a result, the majority of this data has been converted to electronic form. Furthermore, thanks to the internet, this information is now widely disseminated. Authorized users can now use computer networks to communicate and retrieve data from afar. Although the three security goals listed above—confidentiality, integrity, and availability—remain critical, they now have new dimensions. Not only must the computers containing the data be secure, but the network must also be secure.

A network administrator's provisions and rules for preventing and monitoring illegal access, misuse, modification, or denial of a computer network and network-accessible resources are known as network security. In terms of network security, cryptography is a crucial technology. The science and art of changing signals to make them secure and impervious to attacks is referred to as cryptography. Symmetric-Key Encryption, Asymmetric-Key Encryption, and Hashing are the three mechanisms used in cryptography. Asymmetric-Key Encryption employs two keys: one public key and one private key, whereas Symmetric-Key Encryption uses a single secret key for both encryption and decryption. The data is encrypted using the sender's public key, and the message is decrypted using the receiver's private key. Hashing creates a fixed-length message digest from a variable-length message and transmits both the message and the digest, ensuring data integrity.

Despite the fact that several approaches have been created to assure network security, network dangers continue to exist. As a result, a great deal of research is being done in the field of network security.

Cryptography is a method of ensuring message confidentiality. In Greek, the phrase has a special meaning: "hidden writing." Nowadays, however, individuals and organisations' privacy is protected by high-level cryptography, which ensures that information delivered is secure and only the authorised receiver has access to it. Cryptography is a traditional method that is continuously being explored, with historical roots. Examples date back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as additional evidence from ancient Greece and Rome, such as secret writings and the renowned Caesar cypher.

Hundreds of millions of people use cryptography on a regular basis to protect data and information, while the majority are unaware of it. Cryptographic systems, in addition to being incredibly valuable, are also extremely brittle, as a single programming or specification error can compromise them.

We live in an information age, which necessitates the storage of data on every element of our life. This information may be regarded of as an asset, and like any other asset, it must be protected against attacks. Information must be hidden from unauthorised access (confidentiality), protected from unauthorised change (integrity), and accessible only to an authorised entrance when it is needed to be secure (availability). As a result, the three most critical security goals are confidentiality, integrity, and availability.

Computers have unquestionably grown omnipresent in today's world, and as a result, the majority of this data has been converted to electronic form. Furthermore, thanks to the internet, this information is now widely disseminated. Authorized users can now use computer networks to communicate and retrieve data from afar. Although the three security goals listed above—confidentiality, integrity, and availability—remain critical, they now have new dimensions. Not only must the computers containing the data be secure, but the network must also be secure.

A network administrator's provisions and rules for preventing and monitoring illegal access, misuse, modification, or denial of a computer network and network-accessible resources are known as network security. In terms of network security, cryptography

is a crucial technology. The science and art of changing signals to make them secure and impervious to attacks is referred to as cryptography. Symmetric-Key Encryption, Asymmetric-Key Encryption, and Hashing are the three mechanisms used in cryptography. Asymmetric-Key Encryption employs two keys: one public key and one private key, whereas Symmetric-Key Encryption uses a single secret key for both encryption and decryption. The data is encrypted using the sender's public key, and the message is decrypted using the receiver's private key. Hashing creates a fixed-length message digest from a variable-length message and transmits both the message and the digest, ensuring data integrity.

Despite the fact that several approaches have been created to assure network security, network dangers continue to exist. As a result, a great deal of research is being done in the field of network security. It is clear that these studies must be documented in a systematic manner. This document summarises some of the most notable research papers in the field of network security that have recently been published.

II. Literature Review

Susan et al. [1] noted that network and computer security is a new and rapidly evolving technology within the computer science area, with computer security education being a moving objective. Security courses emphasise algorithmic and mathematical topics such as hashing algorithms and encryption. New courses covering the latest types of assaults are published when crackers discover new ways to penetrate network systems, yet each of these attacks becomes outdated daily as new security software responds. Security strategies and abilities continue to emerge in the practise of business, network optimization, security architecture, and legal foundation as security language matures. The essential basic concepts, properties, and purposes of cryptography were demonstrated by Othman O. Khalifa et al. [2]. They highlighted how communication has contributed to the advancement of technology in our day, i.e., the information age, and thus plays a vital role that demands privacy to be secured and assured when data is conveyed over the medium of communication.

Data communication, according to Nitin Jirwan et al. [3], is primarily based on digital data transmission, in which data security is prioritised when utilising encryption techniques to ensure that data reaches the intended users safely and without being compromised. They also exhibited several cryptography approaches, such as symmetric and asymmetric methods, that are used in the data communication process.

Sandeep Tayal et al. [4] stated in a review on network security and cryptography that the rise of social networks and commerce apps has resulted in massive amounts of data being produced daily by organisations all over the world. As a result, information security becomes a major concern when it comes to ensuring the secure transmission of data over the internet. This issue emphasises the need of cryptographic approaches as more people connect to the internet. This paper gives an overview of the many security approaches utilised by networks, including cryptography.

Anjula Gupta et al. [5] discussed the history and significance of cryptography, as well as how information security has become a difficult problem in the computer and communications areas. This paper also provides various asymmetric algorithms that have given us the ability to protect and secure data, in addition to demonstrating cryptography as a way to ensure identification, availability, integrity, authentication, and confidentiality of users and their data by providing security and privacy.

Cryptography, privacy-enhancing technology, legislative developments related to cryptography, reliability, and privacy-enhancing technologies were all discussed in research undertaken by Callas, J. et al. [6].

He stated that the future of cryptography will be determined by how society uses it, which is determined by rules, present laws, and practises, as well as what society wants it to do. He stated that there are many gaps in the realm of cryptography that need to be filled by future scholars. Furthermore, the future of cryptography depends on a management system that generates strong keys to ensure that only the proper individuals with the right keys have access, and that others without the keys do not. Finally, Callas stated that people's perceptions and opinions on security and communication privacy are a reflection of changes in laws enacted in response to events such as the September 11 terrorist attacks.

As a result, cryptography will always play a role in data and information security, both today and in the future.

Moving on to the objectives of cryptography, James L. Massey et al. [7] pointed out that there are two objectives that cryptography seeks to achieve: authenticity and/or secrecy. He explored both Shannon's theory of theoretical secrecy and Simmon's notion of theoretical authenticity in terms of the security it provides (which can be either practical or theoretical).

Finally, Schneier et al. [8] concluded that security secrecy is a fallacy, and that it is not ideal for security to remain hidden, because security that relies solely on secrecy can be vulnerable. It would be impossible to regain that secret if it was lost. In order to provide effective security, cryptography based on short secret keys that can be quickly shared and updated must rely on a basic principle, according to which cryptographic algorithms must be both strong and public. The only sure-fire method to increase security is to open yourself up to public scrutiny.

N. Varol et al. [9] investigated symmetric encryption, which is used to encrypt a specific text or speech. The content to be encrypted is first transformed into an encapsulating chipher that a cypher algorithm cannot understand.

Chachapara, K. et al. [10] investigated secure sharing in cloud computing with cryptography and developed a system that uses cryptography algorithms such as RSA and AES, with AES being the most secure algorithm in cryptography. Users of the cloud can produce keys for various users with varying rights to view their files.

R. Gennaro [11] emphasised randomness in cryptography, explaining that a random process has unknown outcomes, and that this is why randomness is important in cryptography since it allows for the creation of information that an adversary cannot learn or predict.

B. Preneel [12] examined mass surveillance tactics and the security of ICT systems in the post-Snowden age, as well as known ways in which sophisticated attackers might bypass or undermine cryptography.

Sadkhan, S. B. et al. [13] discussed the main processes and trends in cryptography from Julius Cesar's time to the modern era, as well as the current status of Arabic industrial and academical efforts in this field in the past, which are related to existing cryptographic and search for new evaluation methods for information security.

Shouhuai Xu et al. [14] presented new complex systems that may be constructed by utilising trust-based social networks (such as Facebook) to store protected data in a distributed manner and developing specific functional aspects using threshold cryptography.

Without a good batch authentication solution, Lo-Yao Yeh et al. [15] explore peer-to-peer online social networks that are currently vulnerable. As underlying cryptosystems, three new protocols are proposed: one-way hash function, proxy encryption, and certificates. These methods are less computationally expensive than traditional methods.

The topic of defining a standard framework for cryptographic verification of Java and Java-like applications is still open, according to Ralf Kusters et al. [16]. Noninterference features of Java-like programmes can be utilised to give cryptographic

assurances, such as computational indistinguishability and simulation-based security. This is accomplished through the use of Jinja+, a new extended language that builds on Jinja. Jinja is a Java application that gives a lot of features. Its purpose is to offer the necessary structure for cryptographic verification.

Idoia Aguirre et al. [17] provide a hypothetical scenario in which network security experts independently decide on appropriate steps to respond to security alarms in any business network. This study provides a framework for security information and event managers (SIEMs) from various domains to collaborate and make choices in response to security threats, thereby improving corporate network security while dramatically decreasing burden.

Byzantine fault tolerance is a subfield of fault tolerance inspired by the famous two generals' problem, where a small fault in the early stages can burgeon into a more complex and complicated problem. Mai Abdelhakim et al. [18] discuss Byzantine fault tolerance, which is a subfield of fault tolerance inspired by the famous two generals' problem where a small fault in the early stages can burgeon into a more complex and complicated problem. The q-out-of-m rule, which is widely used in distributed detection and can achieve a good tradeoff between miss detection probability and false alarm rate in a computer network, is proposed in this paper. It works as follows:'m' random sensors are polled, and if 'q' of them report 1, the system reports the target as present. Due to the high computational complexity of this strategy, it is not viable for big networks; consequently, this paper proposes a linear q-out-of-m scheme that can be easily applied to large networks. In addition, the research proposes an effective malicious node detection methodology and includes simulation examples to demonstrate the effectiveness of the presented methods.

Mobile Agent is a programme that moves from host to host executing a certain duty, according to Geetha et al. [19]. Each host has a trust and reputation index in Trust and Reputation Management, which is a reputation-based system. TRM for Mobile Agents can construct a secure path, avoiding various common attacks and allowing safe and secure networking with remote hosts.

According to Jesus Tellez Isaac et al. [20], the growth of mobile payment systems has opened the way for the exposure of some security vulnerabilities. Money transfer can be done via SMS, GPRS, RFID, and other methods, although there are some security concerns. One of the major problems is that the keys created by public-key cryptography are excessively large, which adds to the overhead. Elliptic Curve Cryptography (ECC), a new type of cryptography, is introduced to help bypass this difficulty. Another ongoing issue discussed in the article is limited internet connectivity, in which the merchant does not have internet access at the moment of payment, exposing the system to security concerns. The study continues by stating that in the future years, the number of m-payment users and m-payment transactions will explode, and security in these m-transactions will remain a top priority.

According to Kui Ren et al. [21], data saved in the cloud is particularly vulnerable and must be secured. However, efficiently discovering and utilising encrypted data is a significant challenge. The proposed solutions include searchable encryption approaches, which allow users with suitable tokens to browse through data without first decrypting it, lowering overhead dramatically. The study then goes on to describe why some issues with safe multi-keyword semantic search, secure query, and search in non-textual material like graphs still exist. Another serious flaw is that data integrity and availability in the cloud are not guaranteed. The article indicates that more work remains to be done before a secure public cloud environment can be realised.

Sakir Sezer and colleagues al. [22] explore Software Defined Networking, which is a novel approach to network design, construction, and management. It divides the control (brains) and forwarding (muscle) planes of the network to make each easier to optimise.

A Controller serves as the "brains" of the system, offering an abstract, centralised view of the entire network. Network managers can use the Controller to make and push out decisions on how the forwarding plane's underlying systems (switches, routers) will handle traffic fast and easily. SDN can enable the dynamic nature of future network activities and intelligent applications while cutting operational costs through streamlined hardware, software, and management, according to the research. However, there are other obstacles to be overcome in terms of performance, scalability, security, and interoperability.

Salah I et al.[23] present and study a general cloud-based security overlay network that may be used as a transparent overlay network to provide services like intrusion detection, antivirus, and antispam software, and distributed denial-of-service prevention. The article examines the resiliency, efficacy, performance, flexibility, control, and cost of each of these in-cloud security services.

The validity of nodes in an ad hoc network cannot be ensured, according to Yu Zhang et al. [24]. Hackers take advantage of this aspect by impersonating an active network node in order to carry out malicious actions. A technique based on auditing is proposed. Misbehaving nodes drop packets constantly or selectively, and this approach allows you to detect and isolate problematic nodes in a wireless ad hoc network. The paper defends its proposed approach by stating that it does not require complicated acknowledgement mechanisms and can function with encrypted traffic.

Spoofing attacks in computer networks have grown quite widespread, according to Jie Yang et al. [25], and require a robust algorithm to detect and localise such attackers. Cryptographic techniques like digital signatures can be used to verify a node's identity, but this adds a lot of overhead. To identify spoofing attacks, the recommended method is to use the concept of particular correlation of received signal strength (RSS). The study also suggests cluster-based procedures for determining the number of attackers, with Support Vector Machines (SVM) being used to locate them.

Shiyu Ji et al. [26] highlight the most hazardous wormhole attacks, which are independent of MAC protocols and immune to cryptography. Two or more conspiring attackers capture packets at one point and tunnel them to a remote location for a response. This disrupts RIP in the network, creating a bogus shortest path to the attacker, where packets are forwarded. To identify such attacks, a more complex and reliable mechanism called intrusion detection is proposed.

Mohammed et al. [27] propose utilising a report-based payment structure for multihop wireless networks to encourage node cooperation, manage packet transport, and ensure fairness. Lightweight payment reports are sent to the accounting centre instead of receipts, and indisputable security tokens are maintained in the form of "Evidences," so any node suspected of cheating can be asked to provide its "proof" to be verified.

Udi Ben-Porat et al. [28] describe Distributed Denial of Service attacks, which impair server performance by repeatedly forwarding insignificant packets over the network, affecting not only the host but all clients. The paper seeks to build efficient defence mechanisms against DDoS attacks using one of the most common data structures in Network Systems (Hash Tables). From a security standpoint, this research compares Open vs. Closed hashing.

The quantification of a network's total security is discussed by Nayot et al. [29]. Individual components must be measured in relation to one another in order to achieve this. For this, attack graphs are created, which can be used to determine network weaknesses. When it comes to assessing the causal linkages between network variables, however, models like attack graphs fall short. The concept of Bayesian Attach Graphs is thus introduced in this study. Bayesian graphs are directed acyclic graphs with nodes representing random variables and edges representing conditional dependencies. Following

that, the study provides a risk management methodology based on Bayesian Attack Graphs that allows a network administrator to quantify the security degree of a deployed network.

Walter Cerroni et al. [30] describe the recently developed HTTPS protocol, which adds another authentication layer in the form of TLS encryption between HTTP and TCP, thereby increasing the security of the earlier HTTP protocol. When digital certificates are used in electronic communication, it appears to be entirely safe. The strategies of ARP poisoning are described in this paper as a way for an attacker to interrupt data transfer. As you may recall, the ARP protocol aids in finding a node's physical address when the logical address is known. ARP spoofing is the practise of presenting a defective physical address for a logical address with malicious intent. The paper then goes on to show how an attacker may potentially intercept data flow from an otherwise secure connection in a simple but practical example.

The insecurity of the Digital TV band against Primary User Emulation Attacks is discussed by Ahmed et al. [31]. To make it even more safe, an AES encryption standard can be used. The sync bits of DTV data frames can be used to regenerate the sender signal to identify authorised users, preventing PUE attacks, by providing a shared secret between the sender and receiver. It can also detect malicious activity regardless of whether the principal user is present.

Guilin Wang et al. [32] discuss the Single Sign On protocol, which allows a user to be authenticated by various service providers in a distributed network using a single credential. This paper outlines the Chang-Lee SSO technique, which was previously thought to be entirely safe, and uncovers some of the scheme's flaws. Impersonation assaults might take place in one of two methods. For starters, a rogue service provider might exploit a user's credentials to access his account on other genuine service providers. Finally, by imitating a legitimate user, an outsider without credentials can freely use services. The study then concludes by proposing the use of Ateniese's verifiable encryption of RSA signatures to improve the Chang-Lee scheme's robustness.

Yossi et al. [33] begin by debunking the widely held belief that the internet is solely vulnerable to man-in-the-middle attacks and that different security procedures and protocols established to address this issue are adequate to ensure security. Off path hackers, who cannot intervene or eavesdrop on packets but can impersonate as the host and insert incorrect packets into the network flow, are a lesser known fact about the internet. These so-called off-path hackers primarily serve two purposes. DNS cache poisoning is the first of these. The current challenge-response method is insufficient in providing security in this case. The well-known NAT also has some flaws that can be exploited by astute hackers. TCP injection is the second method, in which an off-path hacker can monitor the IP and port addresses as well as the sequence number in a TCP packet and simply inject bogus packets into an otherwise valid stream. To prevent such off-path hackers, the article concludes by suggesting the use of cryptographic mechanisms in addition to those already in use.

A Group Key Agreement cryptographic approach through which a whole network can share a single secret key independent of network/node failures is discussed by Stainslaw et al. [34]. A GKA can be flexible but inefficient, or efficient but ineffective, but new approaches enable a fault-tolerant GKA to deliver logarithmic-sized messages.

Authenticated key exchanges, such as the Diffe-Hellman Key Exchange, require both security and privacy, according to Andrew et al. [35]. Privacy Preserving Authenticated Key Exchange necessitates features such as forward deniability, session transcripts created from DH exponents, and non-traceability of the peer engaging in message and key exchange.

Wiretap networks are a relatively new model proposed by Ning Cai et al. [37]. The nodes in a network can encrypt the received information from the input links using network coding techniques, which increases security. This concept of network coding is combined with information security in the Wiretap Network. In addition to traditional cryptography procedures, this paradigm involves secret key sharing. It is proposed to build safe linear networks that satisfy the graph-theoretic criterion. The study then explores many classic ways to cryptography in a wiretap network before proposing the rWN, which allows r subnet wiretap users to lawfully access encrypted data.

Takao et al. [38] talk about Wolves and Lambs, who are users of biometrics who purposefully or unintentionally produce false positives. Using a minimum log likelihood ratio based sequential fusion approach, a fusion algorithm is devised to prevent wolves and lambs from tampering with biometrics.

Lane Harrison et al. [39] highlight how visualisation is important not only for expressing large amounts of data, but also for analysis, notably network analysis. Several state-of-the-art visualisation technologies that can perform effective network security analysis are investigated and nicely presented. The research closes by describing how these visualisation tools have unique properties that other techniques lack.

WLAN systems, according to Fan Zhang et al. [40], provide a shared channel for several nodes to communicate; even encrypted data over a wifi network is vulnerable to packet inspection. Traffic Demultiplexing is a new way for shaping traffic to prevent analysis using the MAC virtualization layer, with no perceptible performance or overhead loss.

Daniele et al. [41] discuss Real network flows, which are a useful resource for the academic community and include applications such as network traffic simulation and others. Obfuscation of sensitive data entails anonymizing the data in the flow in order to prevent certain attacks from being used against the flow itself.

Security analysts have a conundrum, according to Andrey et al. [40], because they are mainly unaware of the attackers' motivation. The defensive technique could include heavily strengthening the most valuable nodes while leaving other nodes susceptible, or hardening all nodes but achieving just a moderate level of protection. The study provides a solution in which the rival's strategies are carefully examined and a suitable defence mechanism is implemented.

III. Cryptography Concept

The basic premise of a cryptographic system is to encrypt information or data in such a way that an unauthorised person cannot deduce its meaning. Cryptography is commonly used to send data via an unsecured channel, such as the internet, or to ensure that unauthorised persons do not comprehend what they are looking at in a case where they have accessed the information.

In cryptography, the obfuscated data is known as "plaintext," and the process of concealing it is known as "encryption." The encrypted plaintext is known as "ciphertext." This is accomplished through a set of rules known as "encryption algorithms." Typically, the encryption process uses a "encryption key," which is passed to the encryption algorithm together with the data as input. The receiving side can extract the information using a "decryption algorithm" and the necessary "decryption key".

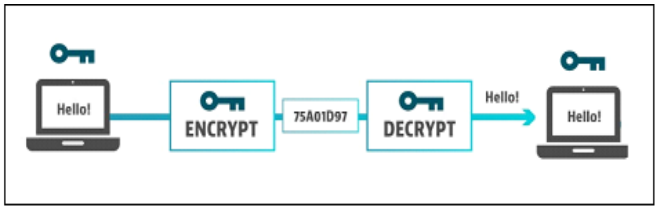

Fig. 1. Cryptography Concept

IV. Conclusion

Authentication, integrity, confidentiality, and no-repudiation are only a few of the major security goals that cryptography helps to achieve. To fulfil these

objectives, cryptographic algorithms are created. The objective of cryptography is to provide reliable, strong, and robust network and data security. We presented a summary of some of the research that has been done in the subject of cryptography, as well as an explanation of how the various algorithms used in cryptography for various security goals work in this paper. In order to protect personal, financial, medical, and ecommerce data while maintaining a reasonable level of privacy, cryptography will continue to be used in IT and business plans.

As the relevance and importance of data privacy grows, so does the importance of network security and cryptography. It is never an absolute procedure to provide network security, but rather an iterative one. As a result, Network Security and Cryptography are currently at the forefront of study.

V. REFERENCES

[1]. S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.

[2]. O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.

[3]. N. Jirwan, A. Singh and S. Vijay , "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 .

[4]. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763770, 2017.

[5]. A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672,2014.

[6]. J. Callas, "The Future of Cryptography," Information Systems Security, vol. 16, no. 1, pp. 15-22, 2007.

[7]. J. L. Massey, "Cryptography—A selective survey," Digital Communications, vol. 85, pp. 3-25, 1986.

[8]. B. Schneier, "The Non-Security of Secrecy," Communications of the ACM, vol. 47, no. 10, pp. 120-120, 2004.

[9]. N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targetting Android Cellphones," in The 5th International Symposium on Digital Forensics and Security (ISDFS 2017), Tirgu Mures, 2017.

[10]. K. Chachapara and S. Bhadlawala, "Secure sharing with cryptography in cloud," in 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, 2013. [14] H. Orman, "Recent Parables in Cryptography," IEEE Internet Computing, vol. 18, no. 1, pp. 82-86, 2014.

[11]. R. GENNARO, "IEEE Security & Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64 - 67, 2006.

[12]. B. Preneel, "Cryptography and Information Security in the PostSnowden Era," in IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity, Florence, 2015.

[13]. S. B. Sadkhan, "Cryptography : current status and future trends," in International Conference on Information and CommunicationTechnologies: From Theory to Applications, Damascus, 2004.

[14]. Shouhuai Xu, Xiaohu Li, Timothy Paul Parker, Xueping Wang, “Exploiting Trust based Social Networks for Distributed Storage of Sensitive Data”, IEEE Transactions on Information Forensics and Security, Volume 6, Issue 1, 2011, pp 39-52, DOI: 10.1109/TIFS.2010. 2093521.

[15]. Lo-Yao Yeh, Yu-Lun Huang, Anthony D. Joseph, Shiuhpyng Winston Shieh, Woei-Jiunn Tsaur, “A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks”, IEEE Transactions on Vehicular Technology, Volume 61, Issue 4, pp 1907-1924, 2012, DOI: 10.1109/TVT.2012.2188821.

[16]. Ralf Kusters, Tomasz Truderung, Jurgen Graf, "A Framework for the Cryptographic Verification of Java-like Programs", IEEE 25th Computer Security Foundations Symposium, Cambridge, MA, 25 - 27 2012, pp 198 -212, DOI: 10.1109/CSF.2012.9.

[17]. Idoia Aguirre, Sergio Alonso, "Improving the Automation of Security Information Management: A Collaborative Approach", IEEE Security and Privacy, Volume 10, No. 1, pp 55-59, January/ February 2012, DOI: 10.1109/MSP. 2011.153.

[18]. Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, Tongtong Li, "Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks", IEEE Transactions on Parallel and Distributed Systems, Volume 25, No. 4, pp 950-959, April 2014, DOI:10.1109/TPDS.2013.74.

[19]. I G Geetha, C Jayakumar, "Implementation of Trust and Reputation Management for Free-Roaming Mobile Agent Security", IEEE Systems Journal, Issue 99, 2014, pp 1 - 11, DOI: 10.1109/JSYST.2013.2292192.

[20]. Jesus Tellez Isaac, Zeadally Sherali, "Secure Mobile Payment Systems", IT Professional, Volume 16, No. 3, pp 36-43, May-June 2014, DOI:10.1109/MITP. 2014.40.

[21]. Kui Ren, Qian Wang, "Security Challenges for the Public Cloud", IEEE Internet Computing, Volume 16, No. 1, pp 69-73, January/February 2012, DOI:10.1109/MIC.2012.14.

[22]. Sezer S, Scott-Hayward S, Chouhan P K, Fraser B, Lake D, Finnegan J, Viljoen N, Miller M, Rao N, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks", IEEE Communications Magazine, Volume 51, Issue 7, pp 36 - 43, July 2013, DOI: 10.1109/ MCOM. 2013.6553676.

[23]. Salah K, Alcaraz Calero, J.M, Zeadally S, Al-Mulla S, Alzaabi M, "Using Cloud Computing to Implement a Security Overlay Network", IEEE Security & Privacy, Volume 11, Issue 1, pp 44 - 53, Feb 2013, DOI: 10.1109/MSP.2012.88.

[24]. Yu Zhang, Loukas Lazos, William Jr. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, Issue 99, pp 1, Dec 2012, DOI: 10.1109/TMC.2012.257.

[25]. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Volume 24, No. 1, January 2013.

[26]. Shiyu Ji, Ting Ting Chen, Sheng Zhong, "Wormhole attack detection algorithms in wireless network coding systems", IEEE Transactions on Mobile Computing, No. 1, pp 1, PrePrints, DOI: 10.1109/TMC.2014. 2324572.

[27]. Mohamed M.E.A Mahmoud, Xuemein (Sherman) Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on parallel and Distributed Systems, Volume 24, Issue 2, pp 209 - 229, 2013, DOI: 10.1109/TPDS.2012.106.

[28]. U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Vulnerability of network mechanisms to sophisticated DDoS attacks", IEEE Transactions on Computers, Volume 62, No. 5, pp 1031 - 1043, 2013, DOI: 10.1109/TC.2012.49.

[29]. Nayot Poolsappasit, Rinku Dewri, Indrajit Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", IEEE Transactions on Dependable and Secure Computing, Volume 9, Issue 1, pp 61 - 74, Feb 2012, DOI: 10.1109/TDSC.2011.34.

[30]. Walter Cerroni, Franco Callegati, "Man-in-the-Middle Attack to the HTTPS Protocol", IEEE Security & Privacy, Volume 7, Issue 1, pp 78 - 81, Feb 2009, DOI: 10.1109/MSP.2009.12.

[31]. Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, Tongtong Li, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks using Advanced Encryption Standard", IEEE Transactions on Information Forensics and

Security, Volume 9, No. 5, pp 772 - 781, May 2014.

[32]. Guilin Wang, Jiangshan Yu, Qi Xie, "Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks", IEEE Transactions on Industrial Informatics, Volume 9, Issue 1, pp 294 - 302, Feb 2013, DOI: 10.1109/TII.2012.2215877.

[33]. Yossi Gilad, Amir Herzberg, Haya Shulman, "Off path hacking: The Illusion of Challenge-Response Authentication", IEEE Security & Privacy, Issue 99, pp 1, Oct 2013, DOI: 10.1109/MSP.2013.130.

[34]. Stainslaw Jarecki, Jihye Kim, Gene Tsudik, "Flexible Robust Group Key Agreement", IEEE Transactions on Parallel & Distributed Systems, Volume 22, Issue 5, pp 879 - 886, May 2011, DOI: 10.1109/TPDS.2010.128.

[35]. Andrew Chi-Chih Yao, Yunlei Zhao, "Privacy-Preserving Authenticated Key-Exchange over Internet", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 1, pp 125 - 140, Jan 2014, DOI: 10.1109/TIFS. 2013.2293457.

[36]. Ning Cai, Raymond W. Yeung, "Secure Network Coding on a Wiretap Network", IEEE Transactions on Information Theory, Volume 57, No. 1, pp 424 - 435, Jan 2011, DOI: 10.1109 /TIT.2010. 2090197.

[37]. Takao Murakami, Kenta Takahashi, Kanta Maatsura, "Toward Optimal fusion algorithms with security against wolves and lambs in biometrics", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 2, pp 259 - 271, Feb 2014, DOI: 10.1109/TIFS.2013.2296993.

[38]. Lane Harrison, Aidong Lu, "The Future of Security Visualization: Lessons from Network Visualization", IEEE Network Magazine, Volume 26, Issue 6, pp 6 - 11, Dec 2012, DOI: 10.1109/MNET.2012. 6375887.

[39]. Fan Zhang, Wenbo He, Yangyi Chen, Zhou Li, XiaoFeng Wang, Shuo Chen, Xue Liu, "Thwarting WiFi side channel analysis through Traffic Demultiplexing", IEEE Transactions on Wireless Communications, Volume 13, No. 1, Jan 2014, DOI: 10.1109/TWC.2013.121013.121473.

[40]. Daniele Riboni, Antonio Villani, Domenico Vitali, Claudio Bettini, Luigi V. Mancini, "Obfuscation of Sensitive Data for Incremental Release of Network Flows", IEEE/ACM Transactions on Networking, Issue 99, pp 1 - 15, Mar 2014, DOI: 10.1109/TNET.2014. 2309011.

[41]. Andrey Garnaev, Melike Baykal-Gursoy, H. Vincent Poor, "Incorporating Attack-Type Uncertainty into Network Protection", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 8, pp 1278 - 1287, Aug 2014.

Cite this article as :

Praful Kr. Ranjay, Prof. Dr. Ramdip Prasad, Arif Md. Sattar, "The Literature Review on The Role and Significance of Cryptography for Network Security in Current Scenario", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 1347-1357, March-April 2019. Available at

Doi : https://doi.org/10.32628/CSEIT2064125

Journal URL : https://ijsrcseit.com/CSEIT2064125