International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 2968–2978

Survey of professional procedures of moving sensitive data using cryptographic methods for securing communication in Wireless network systems

[1]Surendra Talari, [2]G. Jagadish, [3]D. Sateesh Kumar, [4]CH. Suneetha, [5]S. Amiripalli

[1, 4]Department of Mathematics, GIS, GITAM Deemed to be University, Visakhapatnam, AP, India
[2]Department of Computer Science, Anil Neerukonda, Institute of Technology and Sciences, Visakhapatnam, AP, India
[3]Department of Mathematics, Koneru lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India
[5]Department of Computer Science, GIT, GITAM Deemed to be University, Visakhapatnam, AP, India
[1]surendrat.bw@gmail.com,

Abstract

In this paper, Analysts are illuminating how best practices are sent through cryptography calculations and how far these calculations are veered off from practices of utilizing IoT applications on IoT convention stack and related areas to move crude information or delicate information or private information safely by having appropriate assessment and examination done on those convention stacks through legitimate defence exhaustively. To start with, Internet of Things (IoT) suggests giving keen living applications and between associated things equipped for sharing their discernments through the Internet. These gadgets are unique in relation to customary Internet-associated gadgets as in these can perform ability full things all alone with insignificant or no human communication. Second, from the Source client, the information is scrambled utilizing cryptographic calculation and afterward this encoded information is sent alongside profoundly standard arrangement of security conventions. Consequently, the odds of uncertainty a gatecrasher can get that some classified, verification or private information is ruined in the crude information being sent is diminished. What's more, thus, the information sent by the source client to the goal client is made sure about.

Keywords: *sensitive data, cryptography, communication, Wireless IoT, unsecure networks, Wired Networks.*

1. Introduction

Applied Cryptography is the piece of the applied arithmetic field wherein crude information can be encoded and transmitted over the risky correspondence medium then it tends to be unscrambled back to its unique structure. Here the encryption can be set up at the source client before moving it into a risky correspondence medium and in the wake of accepting scrambled message is decoded at the goal client utilizing a mutual key given to it. Prior to the correspondence between source client, middle interpreter, and goal client both of these substances must concur upon symmetric and awry enciphering techniques[1][2] by how they are trading their crude information, it is a Diffie Heilmann key trade method[3]. While data is in travel in unbound media, even the interloper or aggressor gets the data isn't in a reasonable way. There is a need to receive increasingly secure and dependable encryption calculations. The diverse Cryptography and square chain system is one such secure and dependable information security approach[4][5]. Here we studied a few existing strategies have a place with Cryptography and square chain systems where we can utilize numerous applications that can acknowledge different end client who can utilize ehealth the board, remote checking assets by trading crude information as information, for example, content, picture, sound and video with Unicode i.e EBCDIC or ASCII to arrive at more clients around the world. Anyway existing

ISSN: 2233-7857 IJFGCN

methodologies which is length from 1999 to 2020 in the field of cryptography and square chain centers just based around ASCII character set, disregarding non English clients [6].

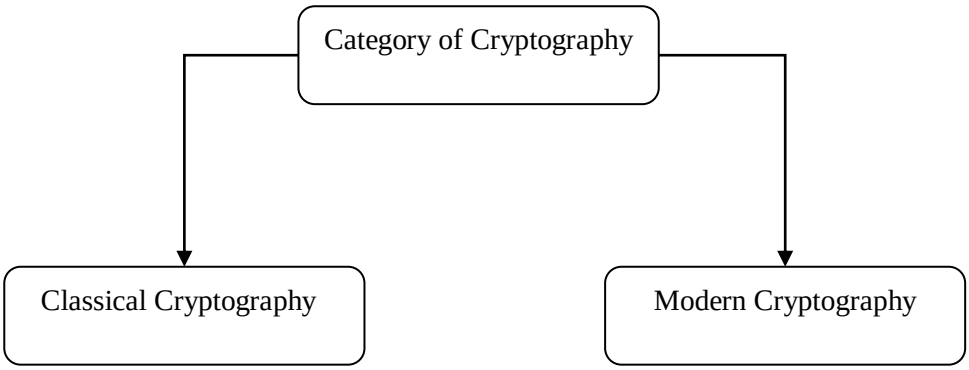

Figure 1. Category of Cryptography

We realised the cryptography in Fig 1, the use of cryptography in internet is increasing day by day not only through computers but also through smart phones, a lot of new technologies and optimized use of resources are expected by an individual or by any organization. Data load will be more on networks and at the same time there are higher chances of capturing, stealing, modifying or cracking of data can be done by an attacker or intruder, which leads to a need of a new technology which can fulfil high storage, randomness nature in generating keys used in encryption as well as decryption by providing more secure and reliable communication [7].

2. Security Problems in IoT

There are various problems identified before we start finding out certain issues found in smart living applications using IoT with cryptography applications:

- Stoppage of carrying Sensitive Data over insecure channel
- escalating Confidential Data, Trade Secrets
- To avoid Misuse of Data.
- Unintentional damage to data, human error, accidental deletion.
- Monetary, Blackmail Purposes.
- Hide Traces of a crime.

In Figure 2 on the above-discovered issues are equipped for taking care of how best ready to determine these issues by utilizing basic accepted procedures to convey crude information or data over the first record. Tragically, it is helpless against even slight information control. There are numerous sorts of cryptography when they are studied exhaustively in the range of 1999 to 2019 for the above kind reference

ISSN: 2233-7857 IJFGCN

.

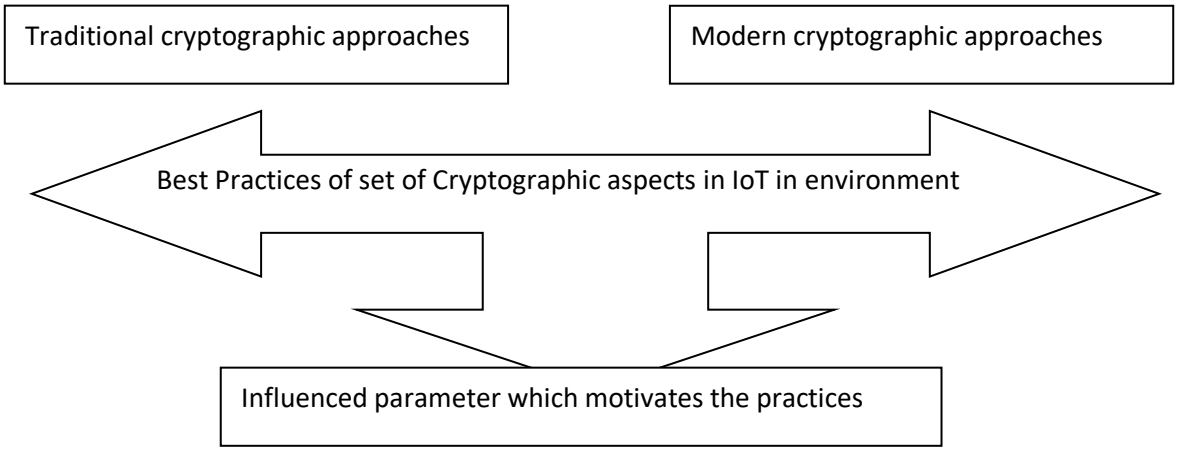

Figure 2. Skeleton of Interconnection of Three entities with practices

3. Best practices of Traditional cryptography aspects

Customary cryptographic viewpoints mean taking care of traditional cryptography which bargains on replacement and transposition philosophies. For instance, supplant one alphabetic with another alphabetic or letters in monoalphabetic replacement procedures. Downpour fence idea to improve letter in downpour fence way. Here numerous old style cryptography calculations were discovered powerless when aggressor utilizes animal power debilitating devices or measurable assaults, discovering design coordinating to get piece of information from cipher text to acquire or obtain entrance for plain content. Best model DNA cryptography is a replacement of letters also [8][9].

Old style cryptography play as significant practices to depend on which data security is investigated by duplicating, catching or composing subordinate; Researchers looked into numerous calculations are fundamentally intended for ruining subtleties from plain content requires substantial hash-based calculations or advanced testaments for web-related exchanges prompts a decent measure of classification, verification, uprightness from which to make it on account of outsider client can't engage the catch subtleties when we utilizing productive calculations is hard to break it. It is hypothetically conceivable to split the cipher text into plain content utilizing savage power assaults or birthday Catch 22 assailants by those individuals utilizing exploitative practices to harm it into the importance type of data before coming to the beneficiary[10],[11].

4. DNA cryptography

DNA Cryptography is bioinformatics with a computer science domain in which lots of researches are happened and happening and it is still expected to come up with a better solution, meeting modern era problems and issues. The technologies under DNA Cryptography which are already accepted are PCR (Polymerize Chain Reaction), DNA synthesis and DNA Digital Coding [12][13]. Here we used DNA Digital Coding technique in which encoding and decoding can be done with the use of binary values such as 0 and 1.DNA Digital Coding is based on biological structure such as DNA (Deoxyribose Nucleic Acid) which is composed of four basic nucleotides such as Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). The proposed system combines the traditional, currently available cryptosystems, uses DNA Digital Coding and maps digital data into biological DNA sequences, and vice versa. The schemes may be deployed to the areas of digital transactions such as credit card/debit card payments, email, SMS (Short Message Service) encryption where users want to have more secure communication[14][15].

ISSN: 2233-7857 IJFGCN

5. Lightweight cryptography

Innovative schemes to solve the problem of creating effective methods and understand means of lightweight cryptography are Use the classic cryptographic algorithms, if it possible. Modification of the classical algorithms with adaptation to the hardware features and limitations of systems at a low cost. Development of new specialized solutions in the methodological, algorithmic and software and hardware terms. Each of these approaches has its drawbacks. Until now, most of the decisions in the field of knowledge refer to the third approach, and show good results. At the same time, however, it should be remembered that the cryptographic algorithm adaptation to the characteristics of the hardware basis with limited resources may have unwanted consequences. They can be expressed in the emergence of additional weaknesses in the algorithm or weakening their overall durability[16].

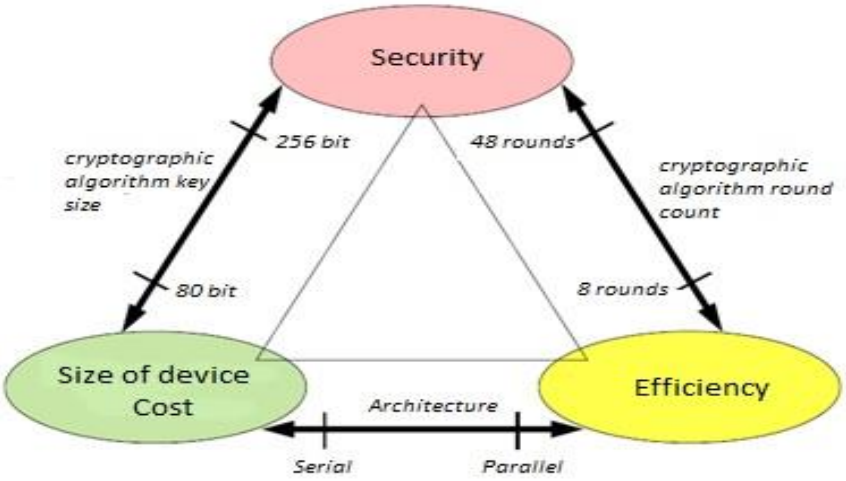

Figure 3. Constraints for lightweight cipher

Initially, it is an endless quest for a harmony between unwavering quality, execution and cost. The key size of square figure decides the proportion of the dependability/cost, the quantity of rounds of encryption - unwavering quality/execution and highlights of the equipment configuration/cost/execution. When in doubt, any two of the three plan objectives can be handily accomplished, while meeting every one of the three necessities referenced in Fig 1, an incredibly troublesome errand. For instance, it is conceivable to give a satisfactory harmony among unwavering quality and execution; nonetheless, to actualize such calculation will require an enormous zone on the circuit, which prompts expanded expense. Then again, it is conceivable to make a dependable and modest framework, however with constrained limit. Also, chip zone is restricted and thirdly, it is critical to control circuits, and in like manner, to characterize the kind of the circuit (dynamic or uninvolved), contingent upon which will force extra prerequisites to the circuit [17] [18].

Are the lightweight encryption calculations not the same as the widespread? There are principle approaches for cryptographers to get undemanding assets with generally solid encryption calculation:

1. Reducing the size of the principle parameters of the calculation: the square encoded information encryption key from 56 piece size key to 256 piece size key and the inside state or instatement vector of the calculation;
2. Attempts to make up for automatic loss of opposition because of the structure of calculations, in view of all around contemplated, ordinarily utilized tasks did by basic straight/non-direct transformation. Such tasks can be introduced as a feature of an architect from which cryptographers "gather" calculation has the correct characteristics;
3. The utilization of "modest" as far as asset utilization, yet the change effectiveness, for example, the control bits stage (which chooses a specific alternative stage contingent upon the

ISSN: 2233-7857 IJFGCN

estimation of the control bit, this bit can be, for instance, a specific piece of the key), move registers, etc;

4. Use of changes for which the encapsulations are conceivable relying upon the specific asset encoder (e.g., diminished memory necessities, yet to the detriment of encryption speed, or the other way around).

It ought to be noticed that the lightweight encryption calculations are made either for a low or medium degree of security or for frameworks, which will consider the points of interest of the calculations and the arrangement that will be found to permit the execution of a calculation to make as sheltered as workable for its degree of opposition [19]. One of the essential ideas that are utilized to consider the lightweight cryptography calculations is GE - entryway equal (the comparable rationale door). This worth is the estimation unit, which permits you to characterize the intricacy of the creation innovation, paying little mind to the multifaceted nature of advanced electronic circuits [20].

6. Modern Cryptography

In current trends, most of the security analysts using modern cryptography techniques. Modern Cryptography is the way of enciphering and deciphering data and information with a secret key to make plain text in mangled form for the attackers. Modern Cryptography can provide good security to the exchange of information; it is also true that in most occasions a really determined attacker can find ways to defeat even the most secure cipher, given enough resources (ultimately money) and/or time. Important security considerations in a cryptography system are trustworthy by using authentication, confidentiality, integrity and no repudiation. Consider the following terminologies being used [21].

The survey basics from 18th century where the mat calculator is used to perform additions and subtractions operations and then Scientist found printing machines and punch-card machines, 19th century, and the advent of computers usage spread across over continental to carry voice conversation details, and using computer network getting more incredible works in World during the 21st century, the go on having more inventions launched to carry digital data methodologies used to carry out hidden message travelled across continentals and contains high computations related to mathematics and its applications [22].

- **Sender s:** Service provider generates data for the receiver.
- **Receiver r:** Intended destination receives and consumes the data from creator.
- **User Text:** It is user understandable form English typed form with grammatically good can transmit to the transmission media.
- **Enciphering Text:** It is indelible form to get it transmission media.
- **Key Usage:** It is process of action to encrypt the English into indelible form with appropriate positions.
- **Enciphering Function:** It is a function to translate the input language into un understanding form which gives ambiguity to the attackers.
- **Deciphering:** it is a reverse function to reverse back into unambiguous form using deciphering process.

ISSN: 2233-7857 IJFGCN

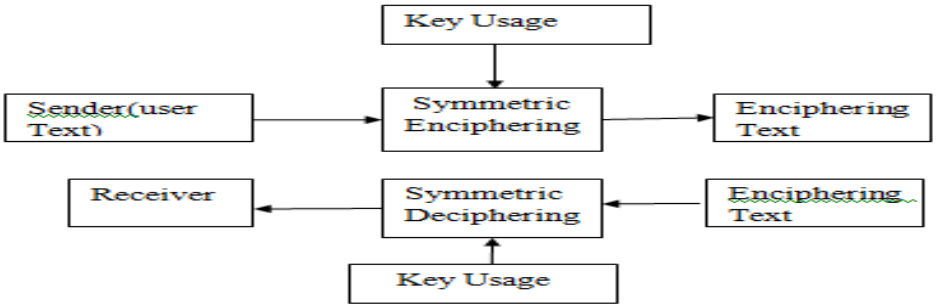

Figure 4. Illustration of Modern Cryptography

7. Secure Information Theoretical approach conceived by Shannon

Definition: A cipher (E,D) over (Key, Plain Text, Cipher Text) has perfect secrecy if for all values of $m_0, m_1 \in M$ ($|m_0| = |m_1|$) and For all values of c belongs to C such that $P_r[E(k, m_0) = c] = P_r[E(k, m_1) = c]$ where k K.

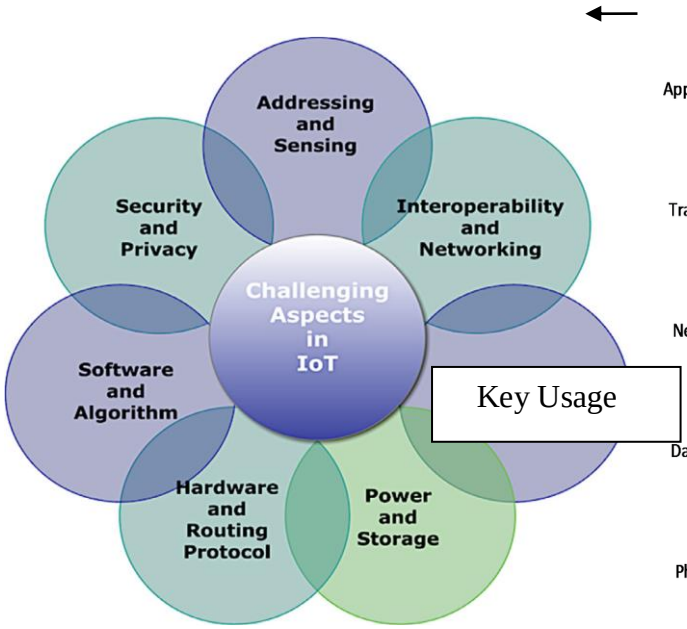

Figure 5a.IoT Challenges in connection with cryptographic aspects

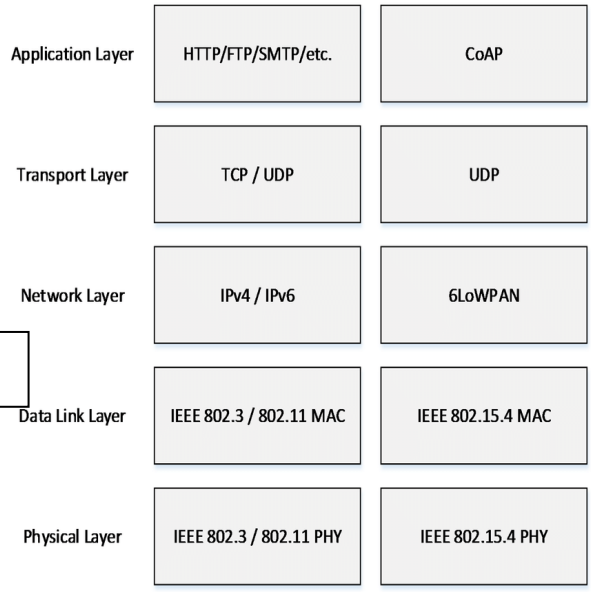

Figure 5b.Comparison of protocol stacks in TCP/IP vs IoT

There is a require to build up an overall secure model for the successful organization of these remote or wired equipment conditions and to manage new difficulties acquainted due with the union of existing cryptographic angles to come out productive age processing advancements. It very well may be by implication said that every remote hardware, i.e IEEE 802.11/IEEE 802.16 in the IoT system ought to be given a similar significance from the point of view of security on the grounds that while assume control over the system, assailants like to constrain passage by abusing the firmware and passwords of the pitifully designed gadgets [23][24]. The IoT convention stack can be envisioned as an augmentation of the TCP/IP layered convention model and is involved the accompanying layers: physical layer, connect layer, arrange layer, transport layer, application convention layer, and application administrations layer. Contrasting the layer stack in TCP/IP connect with IoT arrange Current Researchers are putting forth attempts to build up a design that isn't just protected systems

ISSN: 2233-7857 IJFGCN

however would likewise have the option to forestall the entrance into the system regardless of whether assailants some way or another barge in the framework. A significant advance towards this exertion is the foundation of secure cryptographic conventions that are equipped for guaranteeing information and correspondence protection. Not at all like conventional cryptographic conventions that need inexhaustible assets, these novel conventions are light-weight, which implies that there stay enough assets considerably after the execution of cryptographic calculations. The difficulties that are gone up against by observing fig 3., where IoT explicit cryptography is some way or another like those looked by the customary web based TCP/IP convention suite[25][26].

These incorporate client validation and approval, and the classification and trustworthiness of information during transmission and capacity. For the most part, security arrangements identified with cryptographic components are ordered into two significant classes – symmetric and awry key cryptography. Thinking about the asset limitations, analysts are attempting to locate the one that is reasonable for IoT gadgets. Uneven key systems are all the more impressive; however they devour more force too. In the writing review, endeavours have been put to make cryptographic perspectives like Data Encryption Standard (DES) with 256 bits quality key-size, Advanced Encryption Systems (AES) with 1024 piece quality key size, lighter by diminishing the time and measure of calculations [27]. These conventions depend on the Discrete Logarithm (DL) and Integer Factorization (IF) issue. Based on how troublesome an issue has been taken during the detailing, it is chosen whether the recipe is increasingly impervious to assaults or not. The fundamental centre territory of scientists is to grow progressively productive and secure calculations [28].

8. Motivation

In the last couple of years, a number of research surveys have come out that address the existing security issues in IoT [26]. In these surveys, various challenges are addressed related to smart grids, smart cities, smart healthcare, and smart transport system. In addition to these challenges, issues like confidentiality, availability and integrity are also discussed. However, only few of them discuss the countermeasures to these existing problems. Meanwhile, new challenges and threats are also arising due to quantum computers. Among all the similarities in the existing surveys, the most common is that they are more focused towards the cryptographic techniques that are not able to resist the impact of Quantum Computing. The sub-area of cryptography, i.e., post-quantum cryptography, has drawn the attention of the regularized bodies throughout the world. In the year 2016, National Institute of Standards and Technology (NIST) announced a call for proposals for their aim towards standardization of post-quantum cryptosystems. By taking these efforts into consideration, we follow a top-down approach in this paper to first unfold the security challenges faced by the IoT infrastructure and then discuss the limitations of existing cryptographic techniques. Lastly, we cover different techniques that are suitable for post-quantum IoT world. Although their existence seems a distant future, researchers and organizations are actively involved today in their development.

Cause/Attack type	**Effect**	**Attack Analysis**	**Best Practices**	**Example /Application**
Data Exhilaration	Obfuscation Of Encrypted Data	Loose confidentiality	System admins need to keep track of application usage to identify and block access to unauthorized applications.	Enable Multifactor authentication like biometrics
Data Elicit	Knowledge Is Sought Directly From Human Beings	Loosing Confidentiality	Need to keep changing the document requirements, attributes and keep all information up to date in	Update patches periodically like Operating system upgradation

ISSN: 2233-7857 IJFGCN

			order to remain traceable during testing and verification.	
Dumpster Diving	Looking For Treasure In Someone Else's Email Trash.	Loosing Integrity and Availability	Put hidden restriction on the innocent information like a phone list, calendar, and organizational chart can be used to assist an attacker who using social engineering techniques to gain access to the network.	Sysadmins Keep monitoring on Botnet, Keyloggers and rootkit malware programs
Piggybacking And Tailgating	Cyber Criminal Intentionally Tags Along With Authorized User In Social Network For Entry Into Company Profile.	Loosing Integrity	Identify user who did culprit or misbehaviour on social network.	Avoid spyware program while running original application in web sites. Avoid adware periodically
SEO Poisoning	Cyber Criminals Intentionally Increase Web Site Ranking Upto Higher In Their Own Malware Based Websites.	Legitimate users suffers from Un availability to actual websites	Identify the spyware or malware based web sites who hold social engineering principles.	Sysadmins use anti hack tool kits to avoid endangered websites.
Man In Middle Attacks	Victim Receive Page From Attackers Choice, Those Who Requested.	Attackers alter the real page from original web site	Identify the TCP finger prints and Trace the route.	Using Anti hacker tool kit
Brute Force Attack	Attackers Tries Several Possible Passwords To Crack Legitimate Users Accounts.	Involves word list file contains many 1 billion patterns of passwords	Getting list file and rainbow file and understand the list from dictionary	Using password cracking tools to guess what passwords commonly encountered and eliminate and thwart that mentioned file.
Phishing	Asking Details By Fraudulent User Instead Of Genuine User	Involves installing malware on the victims computer	Ethical hackers need to check periodically by Getting malware programs by tricky way	Using anti spam filters to avoid fraudulent calls.
Sql Injection	Explore Vulnerability By Insert Sql Instruction	Makes the system not to filter the user input correctly for characters in an SQL statement.	Ethical hackers validate inputs properly by recheck whether any Unauthorized SQL scripts running in back ground.	Nikto, Kismet tools used to identify web related vulnerabilities.

ISSN: 2233-7857 IJFGCN

Conclusion

With the appearance of security stages, things that are being utilized in our regular day to day existences have gotten fit to speak with one another utilizing the Internet. Be that as it may, with the utilization of various inbuilt advances, comes different issues among which security issues are of significant concern. So as to manage these issues, different cryptographic natives have been concocted. In any case, with the appearance of best practices, these cryptographic calculations are not dependable enough. Subsequently, it is required to create cryptographic arrangements that would give the normal degree of security in the wired/remote systems. In this paper, we talked about the prescribed procedures of various kinds of systems in detail alongside the related difficulties and existing strategies. A short time later, a nitty-gritty depiction of the regular cryptographic methods has been given. In the later areas, the idea of customary cryptography has been presented. The circumstances and logical results issues talked about in this paper are the principle classifications of the prescribed procedures of cryptographic strategies and it is accepted that these issues are difficult to be tackled in present-day PCs just as in IoT related PCs. Henceforth, so as to limit the assaults created from programmer based PCs, it is important to leave the cryptographic calculations dependent on the customary cryptographic issues and there is a need to adjust and create calculations that depend on present-day cryptographic methods and can oppose the assaults in the wired or remote web world.

References

1. Ya-Fen Chang, et al., paper titled., "An intelligent context-aware communication system for one single autonomic region to realize smart living", published in Elsevier, Information Fusion 21 (2015),PP 57–67.

2. S. S. Amiripalli, V. Bobba, “A Fibonacci based TGO methodology for survivability in ZigBee topologies”. INTERNATIONAL JOURNAL OF SCIENTIFIC &TECHNOLOGY RESEARCH, 9(2), pp. 878-881. 2020.

3. Amiripalli, S. S., & Bobba, V. (2018). Research on network design and analysis of TGO topology. International Journal of Networking and Virtual Organisations, 19(1), 72-86.

4. Amiripalli, S. S., & Bobba, V. (2019). Trimet graph optimization (TGO) based methodology for scalability and survivability in wireless networks. International Journal of Advanced Trends in Computer Science and Engineering, 8(6), 3454-3460. doi:10.30534/ijatcse/2019/121862019.

5. Amiripalli, S. S., & Bobba, V. (2019). An Optimal TGO Topology Method for a Scalable and Survivable Network in IOT Communication Technology. Wireless Personal Communications, 107(2), 1019-1040.z

6. Amiripalli, S. S., & Bobba, V. (2019). Impact of trimet graph optimization topology on scalable networks. Journal of Intelligent & Fuzzy Systems, 36(3), 2431-2442.

7. S. S. Amiripalli, V. Bobba, “A Fibonacci based TGO methodology for survivability in ZigBee topologies”. INTERNATIONAL JOURNAL OF SCIENTIFIC &TECHNOLOGY RESEARCH, 9(2), pp. 878-881. 2020.

8. Kamalesh, V. N., Shanthala, K. V., Ravindra, V., Chandan, B. K., Pavan, M. P., & Bomble, P. P. (2015). On the design of fault tolerant k-connected network topologies. Int. J. Innov. Manag. Technol, 6(5), 339-342.

9. Du, H., Fan, J., He, X., & Feldman, M. W. (2018). A Genetic Simulated Annealing Algorithm to Optimize the Small-World Network Generating Process. Complexity, 2018.

ISSN: 2233-7857 IJFGCN

10. Bannapure, M., & Patil, V. L. (2014, December). Ant Colony Optimization for random network. In 2014 IEEE Global Conference on Wireless Computing & Networking (GCWCN) (pp. 41-46). IEEE

11. Firoozbahrami, M., & Rahmani, A. M. (2012). Suitable Node Deployment based on Geometric Patterns Considering Fault Tolerance in Wireless Sensor Networks. International Journal of Computer Applications, 975, 8887.

12. Panigrahi, D. (2011, January). Survivable network design problems in wireless networks. In Proceedings of the twenty-second annual ACM-SIAM symposium on Discrete Algorithms (pp. 1014-1027). Society for Industrial and Applied Mathematics.

13. M. Pal, P. Sahu and S. Jaiswal, "LevelTree: A New Scalable Data Center Networks Topology," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India, 2018, pp. 482-486, doi: 10.1109/ICACCCN.2018.8748304.

14. [14]Vestin, J., & Kassler, A. (2016, June). Resilient SDN based small cell backhaul networks using mmWave bands. In 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) (pp. 1-3). IEEE.

15. Bao, N. H., Su, G. Q., Wu, Y. K., Kuang, M., & Luo, D. Y. (2017, July). Reliability-sustainable network survivability scheme against disaster failures. In 2017 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 334-337). IEEE.

16. Lloret, J., Garcia, M., Bri, D., & Diaz, J. R. (2009). A cluster-based architecture to structure the topology of parallel wireless sensor networks. Sensors, 9(12), 10513-10544.

17. Amiripalli, S. S., Kumar, A. K., & Tulasi, B. (2016, February). Introduction to TRIMET along with its properties and scope. In AIP Conference Proceedings (Vol. 1705, No. 1, p. 020032). AIP Publishing LLC.

18. Amiripalli, S. S., Kollu, V. V. R., Jaidhan, B. J., Srinivasa Chakravarthi, L., & Raju, V. A. (2020). Performance improvement model for airlines connectivity system using network science. International Journal of Advanced Trends in Computer Science and Engineering, 9(1), 789-792. doi:10.30534/ijatcse/2020/113912020

19. Geyer, F. (2017, December). Performance evaluation of network topologies using graph-based deep learning. In Proceedings of the 11th EAI International Conference on Performance Evaluation Methodologies and Tools (pp. 20-27).

20. Shai, O., & Preiss, K. (1999). Graph theory representations of engineering systems and their embedded knowledge. Artificial Intelligence in Engineering, 13(3), 273-285.

21. Ramiah Chowdary, P., Challa, Y., Jitendra, M.S.N.V. (2019).“Identification of MITM Attack by Utilizing Artificial Intelligence Mechanism in Cloud Environments” Journal of Physics: Conference Series, 1228 (1),012044.

22. Thota, J.R., Kothuru, M., Shanmuk Srinivas, A., Jitendra M, S.N.V. (2020) “ Monitoring diabetes occurrence probability using classification technique with a UI” International Journal of Scientific and Technology Research, 9 (4), pp. 38-41.

23. Amiripalli, S.S., Venkatarao, R., Jitendra, M.S.N.V., Mycherla, N.M.J. (2020) “Detecting emotions of student and assessing the performance by using deep learning” International Journal of Advanced Trends in Computer Science and Engineering, 9 (2), pp. 1641-1645.

ISSN: 2233-7857 IJFGCN

24. Jitendra, M.S.N.V., Radhika, Y. (2020). "A review: Music feature extraction from an audio signal" International Journal of Advanced Trends in Computer Science and Engineering, 9 (2), pp. 973-980.

25. Wu, X., Cao, Q., Jin, J., Li, Y., & Zhang, H. (2019). Nodes Availability Analysis of NB-IoT Based Heterogeneous Wireless Sensor Networks under Malware Infection. Wireless Communications and Mobile Computing, 2019.

26. S S Amiripalli,M S N V Jitendra,Surendra T,Sannith Akkireddi,D Sateesh Kumar ,Design and Implement an Artificial Intelligence based Zombie's Application using Unity3D, "Test Engineering and Management", page numbers 16541 - 16547, volume 83, April, 2020.

27. CH. Suneetha,D. Sravana Kumar,T. Surendra,CH. Neelima,D Sateesh Kumar, Elliptic curve cryptography with special focus on reduction of the cipher size of ECC using Chebyshev Polynomial, "Test Engineering and Management", page numbers 13645-13654, volume 83, April, 2020.

28. S S Amiripalli, T Surendra, Venkata Dileep B, E.V. Priyadharshini, V.Lakshmi Charan Reddy, D Sateesh Kumar Analysis of Airline Connectivity using Network Science, "International Journal of Psychosocial Rehabilitation", page numbers 5229-5234, volume 24/6, April, 2020.

29. Anusha S, Srinivasa Kumar B, Satish Kumar D, *Growth trends in production and export of Indian spices using LOESS approach,* *Test Engineering and Management* ***The Mattingley Publishing Co., Inc,*** January-February 2020 ISSN: 0193-4120 Page No. 12842 – 12853

30. Kocharla L, Rao K, Kumar D, Secure Data Packet transmission over Wireless Sensor Network using security Architecture, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018,

31. Satiskumar et.al, IOT based water level and quality monitoring system in overhead tanks. International Journal of Engineering & Technology. 7. 379. 10.14419/ijet.v7i2.7.10747

ISSN: 2233-7857 IJFGCN