WATERMARKING TECHNIQUES FOR ROYALTY ACCOUNTS IN CONTENT MANAGEMENT WEBSITES FOR IOT IMAGE ASSOCIATION

Siddhartha Vadlamudi, Xandr, USA
Md. Aminul Islam, East Delta University, Bangladesh
Md. Shakawat Hossain, Jagannath University, Bangladesh
Alim Al Ayub Ahmed, Jiujiang University, China
ABM Asadullah, International Islamic University Malaysia, Malaysia

ABSTRACT

Utilizing IoT associations has been trending recently. They have been used in numerous fields of life, comprising protected and subtle segments like the healthcare and military. Images that are used across IoT platforms infringe copyright strategies and rescind the authenticity of the images taken with hard work by a human. Thus, the objective of this study is to provide IoT association of images (pictures/photos) to pages across content management websites with unique watermarks to account for Royalty to the person/association owning the camera. This model indulges in emerging and registering a distinctive number that exclusively ties up the human and the camera which is getting used in such a way that the photo taken by the person will leave a unique identifier or mark which will make the image copyrighted and uploads to cloud for direct usage on any pages in IoT so that direct revenue of the copyrighted photograph goes to the person who clicked the photo. Our results presented the watermarking method to account for royalty in content management websites for IoT association of images contrary to the work's existing result. Our result assumed that with the watermarking method, royalty can be accounted to the rightful owner of the image during the IoT-associated image.

Keywords: Watermarking Method, CMS, Content Management Websites, IoT Association of Image, Copyright.

INTRODUCTION

The IoT is a defined stratum that interlinks smart devices that are connected to the network (Ammar et al., 2018). These devices received data from the surrounding and direct it to the net to be collated, evaluated, and processed utilizing hi-tech (Gubbi et al., 2013). The internet of things architecture is commonly made up of 3 layers namely, the network layer, the application layer, and the perception layer (Vadlamudi, 2021a). It is the perception layer that has all the hardware devices that interlink at once and set up a network (Manikandan & Subha, 2018). Cordless radar networks are seen as one of the primary facilitating technologies for the perception layer (Lazarescu, 2017; Manikandan and Subha, 2018). The perception layers are made up of low-power radar nodes that have restricted computational and storage capacities, and an influential base station (Pawar & Agarwal, 2017).

Cordless radar networks are utilized in an extensive collection of applications like atmosphere control and monitoring, healthcare schemes, home control, and office automation

(Mahgoub and Ilyas, 2016; Manikandan and Subha, 2018). In this software or application, radar shares their data using the shared cordless avenue (Manikandan and Subha, 2018). As a result of this purpose and restriction mentioned above, they can be susceptible to many numbers of security spasms that can impact the confidentiality and integrity of such data like packet drop, a packet replay, data modification, and false data additions (Kui et al., 2008; Paruchuri et al., 2021; Paruchuri, 2020; Khan and Salah, 2018). By the addition of false data to the network, the invaders can generate fake reports that can be yielded severe impairment or risky effects.

However, it very important to have a countermeasure to filter false data at an early stage, and precisely as possible. Many mechanisms have been created to secure the internet of things from such spasms (Azad et al., 2021). These outcomes differ regarding methods (Ammar et al., 2018). Most of these outcomes utilize software verification, trust-oriented methods, anomaly recognition methods, signature-oriented methods, or watermarking methods (Ganapathy, 2019). Moreover, the majority of these modus operndi have their restrictions and cannot be employed efficiently to offer both integrity and confidentiality. Special hardware is required in software verification methods. The anomaly recognition and trust-oriented methods can undergo a high rate of false data (Illiano and Lupu, 2015). Also, additional steps are involved in the building of distribution of standard manners first. Signature-oriented methods can be seen as computationally multifaceted (Granjal et al., 2015). Whereas watermarking methods are utilized in several applications, they were initially employed to protect multimedia content and relational databases (Hameed et al., 2016).

Numerous investigators have deployed them to safeguard radar data. In the watermarking method, an individual datum is entrenched with a distinct watermark by the radar node prior to sending it. The access point can then validate its integrity. The aforementioned flaws of these methods make them multifaceted (Bartariya and Rastogi, 2016), computationally affluent, and many are application- or context-based (Illiano and Lupu, 2015).

Problem Statement

Images that are used across IoT platforms infringe copyright strategies and rescind the authenticity of the images taken with hard work by a human. This model indulges in emerging and registering a distinctive number that exclusively ties up the human and the camera which is getting used in such a way that the photo taken by the person will leave a unique identifier or mark which will make the image copyrighted and uploads to cloud for direct usage on any pages in IoT so that direct revenue of the copyrighted photograph goes to the person who clicked the photo (Amin & Vadlamudi, 2021). This way the content management system which produces pages can use the images and share the profits established on the outcome of revenue from the visitors visiting the page and liking the content.

The Objectives of the Study

The main input of this article is to provide IoT association of images (pictures/photos) to pages across content management websites with unique watermarks to account for Royalty to the person/association owning the camera. This can filter false added data efficiently and as early as likely devoid of depending on any stationary node setting or secure directing protocols. The study aims to safeguard the integrity, legitimacy, and privacy of corporeal data utilizing a trivial watermarking method. It will offer en route fairly than end-to-end clarifying to curtail communication above by decreasing the quantity of false data reports.

Integrity and legitimacy will be providing by entrenching a watermark at indiscriminate settings within the data. Inserting a watermark within many arbitrary settings will make it more challenging for a rival to inject a false report. The structure will also utilize homomorphic symmetric encryption to offer privacy. The main objective of this article is to discourse the following subjects:

Propose a different and arbitrary method of inserting the watermark that will be according to the pseudorandom number creator algorithm.

This article will be sectioned into five sections; section one is the introduction, Section two will take care of literature reviews of related work by other scholars using different approaches.

LITERATURE REVIEW

A number of researches have been carried out on security-associated matters in the internet of things (Ammar et al., 2018; Ahmadi et al., 2018; Al-Garadi et al., 2018). This review makes available a concise and inclusive system of the present security susceptibilities, and trials that diverse applications witness. Several contemporary forms of study have offered pawn procedures contrary to data addition spasms in the internet of things (Vadlamudi, 2021b). These pawn procedures can be distributed into 5 major groups: software verification, anomaly recognition, trust supervision, signature-oriented methods, and digital watermarking methods. These researchers have engaged clarifications to counter addition spasms on the sensory data of internet of things applications (Vadlamudi et al., 2021). Thus, this review will concentrate on watermarking methods.

Watermark methods are another form of integrity modus operandi. There are 3 classes of digital watermarks; fragile, robust, and semi-fragile watermarks (Lalem et al., 2016). Fragile and robust watermarks have been the subject of investigation in wireless radar networks. Semi-fragile watermarking is not usually applied in wireless radar networks. The study on applying watermarking methods for integrity and verification in wireless radar networks started in 2003. The first watermarking system that inserts cryptographically programmed signatures into data (Fang and Potkonjak, 2003; Ganapathy et al., 2020; Ahmed et al., 2021).

Fragile watermarking is applied to offer data integrity and verification via inserting a watermark into the innovative data. Tiwari et al. (2013) established a hop-by-hop fragile watermarking method. Tiwari and co-authors have presumed the network to be uniform and designed like a tree with individual cluster heads to have at utmost 3 children. The method utilizes data collection to decrease communication above your head. The watermark dimensions are only one bit, and the cohort method is very modest by applying the high-class XOR operator. The inserting is prepared at the slightest important bit of the data. The method is modest but not protected. A cross-layer watermarking-oriented data collection (Boubiche et al., 2015) is an additional fragile watermarking setup that implements 2 forms of watermarks. A fragile watermark is the first form that is deployed to authenticate data directed from the ground state of the network. The higher state of the network that is aggregator nodes employs a reinforced fragile watermark that is more protected as the watermark is encrypted applying the asymmetric key. The mechanism uses a diverse inserting method than most of the recommended systems (Paruchuri, 2021). The inserting position of the watermark will be vibrant, and it will be calculated according to the wakeup interlude applied by the individual node.

While this ensures it fairly arbitrary, it can be easily recognized as it will yield a model. A cross-layer watermarking oriented data collection mechanism also, demands synchronization

among nodes to define the wakeup period. A watermarking algorithm according to a one-way hash task was suggested by Sun et al (2013). The watermarking is calculated for each byte of data and then clustered utilizing the XOR role. The ultimate watermark is then classified among bytes and inserted in predefined terminated galaxies. The recommended algorithm is computationally modest. Moreover, it mainly offers end-to-end integrity.

Hameed et al. (2018) had recommended a zero-watermarking method, which creates a watermark from the assets of the detected data. After encrypting the watermark utilizing a mutual secret key, the radar inserts the encrypted watermark at the end of the detected data before, it is directed to the base station. Zero-watermark methods and the outcomes displayed that it does not introduce any computation overhead as the generation procedure is modest. The zero-watermark method is susceptible to various security openings in the circumstance of revealing the mutual hush-hush key as it utilizes only one key for the entire network.

Watermarking-LEACH (Rouissi and Gharsellaoui, 2017) is another integrity conserving method that increases a watermark on top of the LEACH course-plotting protocol. It changes the original method of LEACH by totaling watermarking inserting at the group heads and watermark isolation at the BS. This method consists of nominal changes to a very renowned channeling protocol. Moreover, it only offers integrity at one portion of the communication that is among group heads and BS. A semi-sightless watermarking method that utilizes linear interpolation to insert the watermark into the data was recommended by Lalem et al. (2016). The major merit of the method is that it does bring together any additional bits for the watermark. Moreover, it utilizes a permanent watermark variable for all nodes in the structure that can be merely cracked. Ren et al. (2015) buttressed the robust watermarking as an instrument to protect copyright and it can also be combined with fragile watermark. Ren and co-authors suggested a digital watermarking system according to multiple roles to secure images transmitted in a wireless radar network. The system inserts 2 forms of watermarks that is the robust and the fragile watermarks, which offer copyright security and integrity respectively.

The robust form is created or generated from the stable properties of the original image, the picture pixels are utilized to create the fragile watermark. The system is only utilized in wireless or cordless multimedia radar networks that deal with visual radar. Guan et al. (2016) recommended different robust watermarking methods for node verification. The recommendation system calculates the watermark according to a randomly selected data sampling period. The system is not robust in recognizing false data embedded spasms, as it does not deliberate all of the data in creating the watermark.

The reversible watermark methods were suggested by Shi & Xiao (2013), Ganapathy (2019), & Ding et al. (2015). Si & Xiao (2013) suggested a reversible watermarking algorithm according to estimation error growth. The algorithm clusters every 2 head-to-head data items together. The first one is utilized to collate the watermark, while the latter is deployed in the carrier for it. The setback of this technique is that authentication is end-to-end, meanwhile, authentication demands additional storage as it uses storage as it practices buffering.

Ding et al. (2015) recommended the same end-to-end or encrypting algorithm that the watermark is generated according to the variance increase. The algorithm clusters n data items and utilizes them all to compute the watermark. The inserting procedure computes the weighted variance between the respective data entry with the first data entry.

The inserting procedure is candid, as every bit of the watermark is inserted in the lowest important bit of respective data entry. The algorithm can make sure the final data retrieval at the base station. Hence, it cannot recognize integrity laterally the path of the communication. Amin &

Vadlamudi (2021) recommended an enhanced version of the variance growth technique utilized by Ding et al. (2015). The entire network was resumed to be viewed as an image with the respective radar node as a pixel. The method makes a sole watermark for all the scheme's data and divided it into various segments. The respective segment is allotted to arbitrary radars for inserting. The isolating operation will utilize a location map to know which radar nodes were selected to insert the watermark. The flaw of the method is that obligation for the watermarking procedure in the respective round is given to a sole node.

METHODS

The planned scheme will offer data integrity, verification, and privacy by inserting watermark at different locations within the data and utilizing systematic encryption. The planned scheme involves 3 phases:

1. Setup and Key Running
2. Recognizing and Reporting, and
3. Authenticating and computation

The groups are produced at the set and key running phase, and all the verification data is allotted to the radars at the first phase. Thereafter, according to periodic recess, radar nodes will commence to sense info, encrypt it, inserted the watermark at an arbitrary location, and then send the end report (Ri) to the group head to commence the authentication step.

In phase two, the group or the cluster head checks if the received information is legal or not to screen bogus packets. The authentication is carried out by reinforcing the watermark from the secluded data. For each legal data of the received information, CH computes the sensed data, inserts a new watermark in the computed data, and sends it to the access point. The AP discretely decrypts and authenticates the information or reports of the respective cluster, as it is expected, that the AP has all of the needed keys and variables.

ENCRYPTION ALGORITHM

The encryption algorithms are generally costly and complex to calculate, but we have tried using a trivial encryption algorithm that was suggested by Castelluccia et al. (2009). The encryption role is as presented below;

$$c = Enc(d, k, M) = d + k(modM),$$

Where d is the data to encrypt, k is the stealthy key for the node, and M is the modulus.

WATERMARKING ALGORITHM

The essential objective of the studied watermarking algorithm is to arbitrarily insert the watermark within the data and at the same time manage to isolate or separate it. Also, robust watermarking tries to affirm and efficiently sustain the energy level of the nodes. The algorithm involves 2 processes namely, watermark generation and inserting. "The watermark generation procedure captures sensory data after encryption" E_1 as feedback from the radar node S_1 and generates a watermark, W_1.

The time and radar ID are also utilized as feedbacks to the keyed-hash message verification code (HMAC) to create the outcome watermark. The final watermark is calculated with the formula below:

$$W_1 = Hash((E_1 || Time || S_1ID), k_{cj})$$

Thereafter, the watermark is inserted at arbitrarily terminated cosmoses of the encrypted data E_1 is presented in Figure 1. These terminated cosmoses are resolute by utilizing a pseudo-arbitrary number generator.

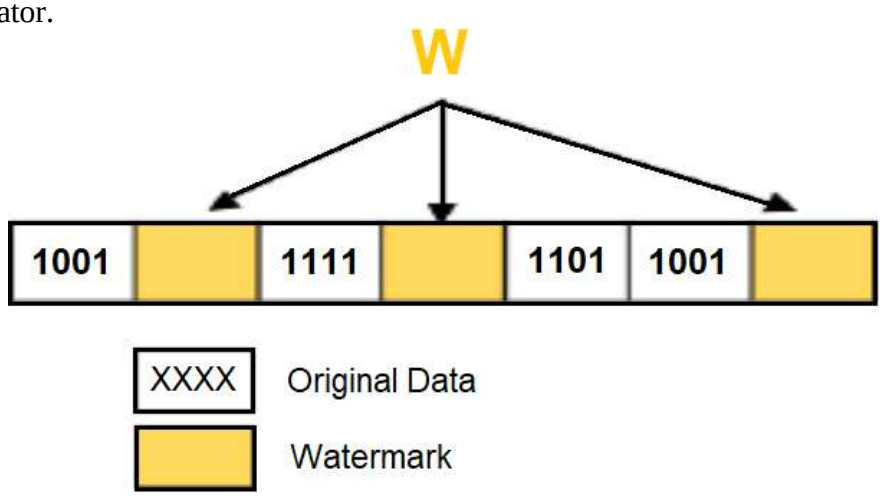

FIGURE 1
DIAGRAM SHOWING ENCRYPTED DATA

The sensor's modules in control for the 2 sub-processes of encryption of data and watermarking cohort are presented in Figure 2.

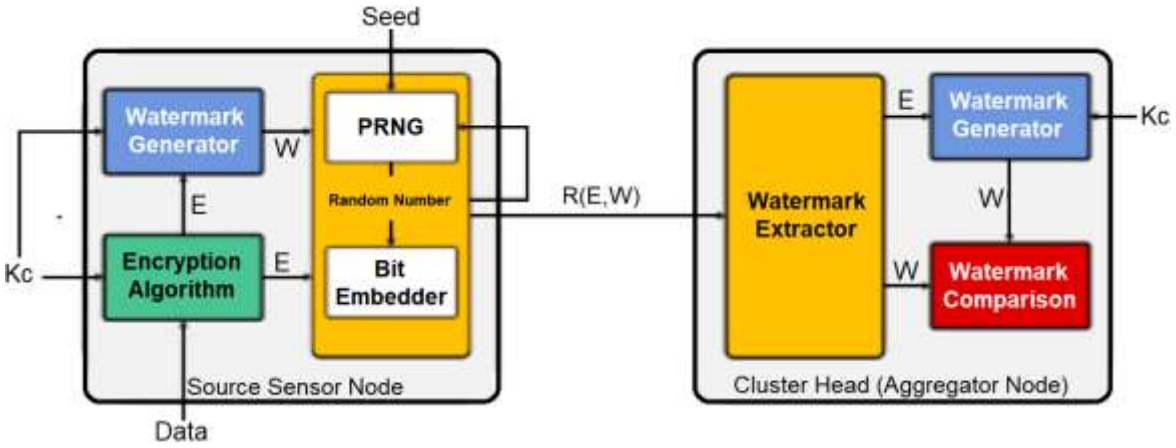

Figure 2
A SCHEMATIC DIAGRAM SHOWING ARBITRARIES WATERMARKING CLARIFYING SYSTEM

A schematic diagram of the arbitraries Watermarking Clarifying System displaying the modules of the radar node and cluster head. It also displays the movement of data among the modules.

There are various techniques to construct "pseudo-random generators (PRNG) "appropriate for use with our scheme. For straightforwardness, we take the "linear congruential generator (LCG)" (Knuth, 1997) (in the following equation to calculate each position of Wi).

$$Xn+1 = (ajXn + cj) \bmod mj.$$

Here, $mj > 0$ is a modulus, aj ($0 < aj < mj$) is the multiplier, cj ($0 \leq cj < mj$) is the growth, and Xn ($0 \leq Xn < mj$) is the present seed.

Each produced Xn+1 is utilized as a pseudo-random number and converts the new seed. Each node calculates 3 values of Xn+1 to utilize as the locations of Wi. To circumvent every cluster having the same number generated for it, each cluster j has different parameters for its pseudo-random quantity creator.

DISCUSSION

In this section, we appraise the presentation of the watermarking method to account for royalty in content management websites for IoT association of images contrary to the work existing result by Cui et al. (2018). We liken their presentation to clarifying dimensions. The simulations of both systems were carried out deploying MATLAB. A diverse wireless radar network comprising of n = 100 nodes is measured in this simulation. The significance of m = 0.1, which denotes that ten percent of the total quantity of nodes are innovative nodes comprising a period more energy than the normal nodes. Screening effectiveness examines the proportion of the quantity of recognized cruel packets to the total quantity of cruel packets. This study assumed that with the watermarking method, royalty can be accounted to the rightful owner of the image during the IoT-associated image. Also, the aggressor recognizes the MAC technique that was utilized to produce the watermark in this study and the MAC scheme that was employed to produce the MAC in the selected case study of Cui et al. (2018) scheme. Consequently, the aggressor can only arbitrarily principles that are underground restrictions of the respective system. For this feature, we have inserted the network with dissimilar numbers of cruel packets and are required to recognize how numerous packets were noticed and forbidden by the system. The proportion of clarifying competence demonstrates that the system can accomplish better.

CONCLUSION

IoT associations show an essential function in constructing new resolutions for numerous real-time difficulties. They link physical radar, field control hubs, and cloud schemes to allow consistent and smart claims. Lately, IoT associations have been being subjected to fabulous industrial importance due to their benefits. Moreover, physical spasms like false insertion spasms are measured to be one of the major pressures for the security of the object in the IoT. False data insertion attacks are measured to be very important in sensor networks where any little change in the data dimension could lead to simple concern. The main objective of this suggested system is to be an energy-efficient device for safeguarding such networks contrary to data addition spasms. We employ a "homomorphic encryption algorithm" to safeguard end-to-end data privacy and a watermark to attain en-route data clarifying. The system utilizes a watermark that is produced and inserted into the unique data directed by all basis nodes in the network.

The watermark is produced according to 4 features containing an encrypted freight, the stealthy mutual key of the group, the radar's sensing, and the data retention time of each radar node. This watermark is then inserted into arbitrary locations inside the packet. We simulated our system and compare the result of this study with the Cui et al. (2018) system. Cui and co-authors' work utilizes a homomorphic MAC role to offer for end-to-end integrity that is computationally costly and it is time-consuming during generation. Our results showed that watermarking method realizes a well computationally effective and consumes less vitality. Consequently, investigation strength should be completed to enterprise a new low-complexity system, yet protected data integrity system that can detect and filter out false data addition spasms.

REFERENCES

Ahmadi, H. Arji, G. Shahmoradi, L. Safdari, R. Nilashi, M. & Alizadeh, M. (2018). The Application of Internet of Things in Healthcare: A Systematic Literature Review and Classification. *Univers. Access Inf. Soc*., 1–33.

Ahmed, A.A.A. Paruchuri, H. Vadlamudi, S. & Ganapathy, A. (2021). Cryptography in Financial Markets: Potential Channels for Future Financial Stability. *Academy of Accounting and Financial Studies Journal*, *25*(4), 1–9. https://doi.org/10.5281/zenodo.4774829

Al-Garadi, M. A.; Mohamed, A.; Al-Ali, A.; Du, X. & Guizani, M. (2018). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. arXiv 2018, arXiv:1807.11023.

Amin, R., & Vadlamudi, S. (2021). Opportunities and Challenges of Data Migration in Cloud. *Engineering International*, *9*(1), 41-50. https://doi.org/10.18034/ei.v9i1.529

Ammar, M.; Russello, G. & Crispo, B. (2018). Internet of Things: A Survey on the Security of Iot Frameworks. *J. Inf. Secur. Appl*., 38, 8–27.

Azad, M.M., Ganapathy, A., Vadlamudi, S., & Paruchuri, H. (2021). Medical Diagnosis using Deep Learning Techniques: A Research Survey. *Annals of the Romanian Society for Cell Biology*, *25*(6), 5591–5600. Retrieved from https://www.annalsofrscb.ro/index.php/journal/article/view/6577

Bartariya, S. & Rastogi, A. (2016). Security in Wireless Sensor Networks: Attacks and Solutions. *Environment*, 5, 214–220.

Boubiche, D.E.; Boubiche, S. & Bilami, A. (2015). A Cross-Layer Watermarking-Based Mechanism for Data Aggregation Integrity in Heterogeneous Wsns. IEEE Commun. Lett. 2015, 19, 823–826.

Castelluccia, C. Chan, A.C.-F. Mykletun, E. & Tsudik, G. (2009). Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks. ACM Trans. Sen. Netw. 2009, 5, 3.

Cui, J., Shao, L., Zhong, H., Xu, Y. and Liu, L. (2018). Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks. *Peer-to-Peer Netw.* Appl. 11, 1022–1037.

Ding, Q.; Wang, B.; Sun, X.; Wang, J. & Shen, J. (2015). A Reversible Watermarking Scheme Based on Difference Expansion for Wireless Sensor Networks. *Int. J. Grid Distrib. Comput*., 8, 143–154.

Fang, J. & Potkonjak, M. (2003). Real-Time Watermarking Techniques for Sensor Networks. In Proceedings of the Electronic Imaging 2003, Santa Clara, CA, USA, 21–24 January 2003; pp. 391–402.

Ganapathy, A. (2019). Image Association to URLs across CMS Websites with Unique Watermark Signatures to Identify Who Owns the Camera. *American Journal of Trade and Policy*, *6*(3), 101-106. https://doi.org/10.18034/ajtp.v6i3.543

Ganapathy, A., Redwanuzzaman, M., Rahaman, M.M., & Khan, W. (2020). Artificial Intelligence Driven Crypto Currencies. *Global Disclosure of Economics and Business*, *9*(2), 107-118. https://doi.org/10.18034/gdeb.v9i2.557

Granjal, J. Monteiro, E. & Silva, J.S. (2015). Security in the Integration of Low-Power Wireless Sensor Networks with the Internet: A Survey. *Ad Hoc Netw*., 24, 264–287.

Guan, T. & Chen, Y. (2016). A Node Clone Attack Detection Scheme Based on Digital Watermark in WSNs. In Proceedings of the IEEE International Conference on Computer Communication and the Internet (ICCCI), Wuhan, China, 13–15 October 2016; pp. 257–260.

Gubbi, J. Buyya, R. Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Gener. *Comput. Syst*., 29, 1645–1660.

Hameed, K.; Khan, A.; Ahmed, M.; Reddy, A.G. & Rathore, M.M. (2018). Towards a Formally Verified Zero Watermarking Scheme for Data Integrity in the Internet of Things Based-Wireless Sensor Networks. *Future Gener. Comput. Syst*., 82, 274–289.

Hameed, K. Khan, M.S. Ahmed, I. Ahmad, Z.U. Khan, A. Haider, A. & Javaid, N. (2016). A Zero-Watermarking Scheme for Data Integrity in Wireless Sensor Networks. In Proceedings of the 19th International Conference on Network-Based Information Systems (NBiS), Ostrava, Czech Republic, 7–9 September 2016; pp. 119–126.

Illiano, V.P. & Lupu, E.C. (2015). Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey. *ACM Comput. Surv*., 48, 1–33.

Khan, M.A. & Salah, K. (2018). Iot Security: Review, Blockchain Solutions, and Open Challenges. *Future Gener. Comput. Syst*., 82, 395–411.

Knuth, D.E. (1997). The Art of Computer Programming; Addison-Wesley: Boston, MA, USA, 1997; Volume 2.

Kui, R.; Wenjing, L. & Yanchao, Z. (2008). Leds: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. *IEEE Trans. Mob. Comput*., 7, 585–598.

Lalem, F. Muath, A. Bounceur, A. Euler, R. Laouamer, L. Nana, L. & Pascu, A.C. (2016). Data Authenticity and Integrity in Wireless Sensor Networks Based on a Watermarking Approach. In Proceedings of the 29th International Florida Artificial Intelligence Research Society, Key Largo, FL, USA, 16–18 May 2016.

Lazarescu, M.T. (2017). Wireless Sensor Networks for the Internet of Things: Barriers and Synergies. In Components and Services for Iot Platforms; Springer: Berlin/Heidelberg, Germany; pp. 155–186.

Mahgoub, I. & Ilyas, M. (2016). Sensor Network Protocols; CRC press: Boca Raton, FL, USA.

Manikandan, N. & Subha, S. (2018). Parallel Aes Algorithm for Performance Improvement in Data Analytics Security for Iot. Int. J. Netw. Virtual Organ., 18, 112–129.

Paruchuri, H. (2020). The Impact of Machine Learning on the Future of Insurance Industry. *American Journal of Trade and Policy*, *7*(3), 85-90. https://doi.org/10.18034/ajtp.v7i3.537

Paruchuri, H. (2021). Conceptualization of Machine Learning in Economic Forecasting. *Asian Business Review*, *11*(1), 51-58. https://doi.org/10.18034/abr.v11i1.532

Paruchuri, H. Vadlamudi, S. Ahmed, A.A.A. Eid, W. & Donepudi, P.K. (2021). Product Reviews Sentiment Analysis using Machine Learning: A Systematic Literature Review. *Turkish Journal of Physiotherapy and Rehabilitation*, *23*(2), 2362-2368, https://turkjphysiotherrehabil.org/pub/pdf/322/32-2-316.pdf

Pawar, M. & Agarwal, J. (2017). A Literature Survey on Security Issues of WSN and Different Types of Attacks in Network. *Indian J. Comput. Sci. Eng*., 8, 80–83.

Ren, Y. Cheng, Y. Wang, J. & Fang, L. (2015). Data Protection Based on Multifunction Digital Watermark in Wireless Sensor Network. In Proceedings of the International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, 21–24 September 2015; pp. 37–41.

Rouissi, N. & Gharsellaoui, H. (2017). Improved Hybrid Leach Based Approach for Preserving Secured Integrity in Wireless Sensor Networks. *Procedia Comput. Sci*., 112, 1429–1438.

Shi, X. & Xiao, D. (2013). A Reversible Watermarking Authentication Scheme for Wireless Sensor Networks. Inf. Sci., 240, 173–183.

Sun, X.; Su, J.; Wang, B. & Liu, Q. (2013). Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks. *Int. J. Secur. Appl*., 7, 407–416.

Tiwari, A. Chakraborty, S. & Mishra, M.K. (2013). Secure Data Aggregation Using Irreversible Watermarking in WSNs. In Proceedings of the Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, India, 26–27 September 2013; pp. 330–336.

Vadlamudi, S. (2021a). The Economics of Internet of Things: An Information Market System. *Asian Business Review*, *11*(1), 35-40. https://doi.org/10.18034/abr.v11i1.523

Vadlamudi, S. (2021b). The Internet of Things (IoT) and Social Interaction: Influence of Source Attribution and Human Specialization. *Engineering International*, *9*(1), 17-28. https://doi.org/10.18034/ei.v9i1.526

Vadlamudi, S. Paruchuri, H. Ahmed, A.A. A. Hossain, M.S. & Donepudi, P.K. (2021). Rethinking Food Sufficiency with Smart Agriculture using Internet of Things. *Turkish Journal of Computer and Mathematics Education*, *12*(9), 2541–2551. https://turcomat.org/index.php/turkbilmat/article/view/3738 x`