Image Association to URLs across CMS Websites with Unique Watermark Signatures to Identify Who Owns the Camera

Apoorva Ganapathy

Senior Developer, Adobe Systems, San Jose, California, **USA**

*E-mail for correspondence: apganapa@adobe.com

Source of Support: None **No Conflict of Interest:** Declared

ABSTRACT

Internet is the world's network of connected computer networks. Internet means an interconnected network. It is a network of connected web servers. Internet helps data and people across the globe. Internet of things refers to network-connected things with embedded computer chips. Things on the internet would include devices enabled for internet access. IoT association of images on content management websites with unique watermark signature to account for Royal to the owner of the picture will help against piracy, copyright infringement, and misuse of photos registered with unique identification keys. This will make content management easier. It will generate revenue for the person who takes the copyrighted picture. A watermark is an embedded signature in a thing. It could be embedded in a video, image, and other file types for distinction and marking for ownership. It could be visible or invisible. It also provides a means to trace a product to the owner. This work looks into how images with watermark can be connected to the IoT for tracking and fighting piracy.

Keywords: Internet of Things (IoT), Watermark, Embed, Unique Identifiers, Copyright, Artificial Intelligence, Content System, Web Server Authentication, Device

INTRODUCTION

Internet of Things (IoT) refers to a network of interconnected computer systems. They can be registered animals or humans with UIDs (unique identifiers). The connected systems can be mechanical or digital and automated devices that are embedded with UIDs. Transfer of data in the IoT is possible within the connected devices without the needing man to man or man to computer communication. To be a Thing in the IoT, there must be a unique identifier. This could be a biochip with a transponder implanted in an animal for tracking or a health implant in a human with a chip. A machine with advanced artificial intelligence can detect faults for maintenance, like a sensor in cars that can detect faults and warn the driver of such fault. Internet protocol address (IP address) can also be assigned to an inanimate object or device to connect it to the IoT and allow for data transfer using the IoT network (Ganapathy, 2018). The IoT allows for connection between the IoT things, which enables a better understanding of the Things in the network. Largely, more organizations employ the benefits of the IoT to increase customer service, make efficient decision-making systems, and improve business value.

THE INTERNET OF THINGS

The IoT network comprises systems and a network of web-connected intelligent devices that employ encoded networks like sensors, processors, and interactive hardware to receive, send and store data. The network in the IoT uses the stored data. To use the stored data, the IoT device sends out the collected sensor information through a connection with a gateway on the IoT or through other means such as using devices with edge tools where data is either sent for analysis on the local network or in the cloud. Connected devices on the IoT network interact with each other and use the shared data they acquire to solve problems. The interactions within the network are done without human supervision or interference, and most of the job is carried out by the devices. Even though humans may communicate with the devices for setting them up, writing scripts for protocols and commands provides access to information. The Different applications used by IoT decide the protocol and system of connection, communication, and network which the things or devices are to use. Artificial Intelligence (AI) and machine learning in IoT improve data collection and processing by the connected devices in a network system.

Machine learning makes it dynamic.

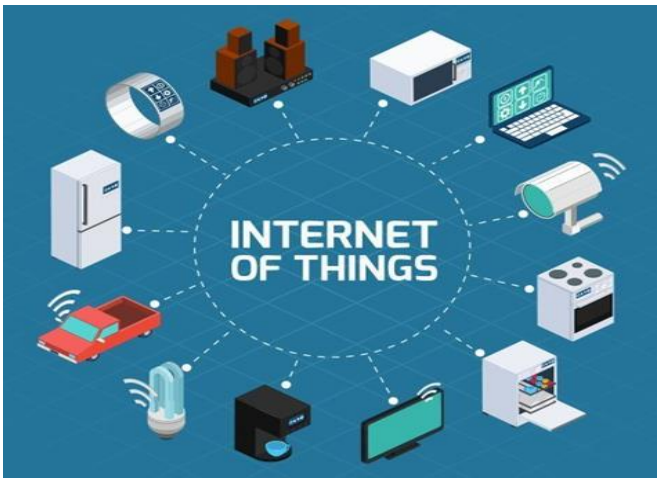

Figure 1: IoT (Source: engalaxy.com)

The IoT importance

The Internet of Things connects the various things on the internet, making it easier to live and allow jobs to be done more smartly. It also gives total control to the users.

Also, for business enterprises, IoT gives a real-time analysis of their systems' performance and provides examinations into everything regarding the functions of the devices in the supply network and logistics. This makes IoT important for enterprises. IoT through artificial intelligence and machine learning reduces labor costs by automating jobs and processes for companies. It reduces waste and makes service delivery more efficient. In the long run, client transactions become more transparent, and the cost of production and delivery reduces remarkably.

The IoT currently plays a very crucial role in our everyday life and remains a vital technology. It would keep developing into a more advanced level as more business enterprises and people use it. More people would get to understand the need for a connected network of the device.

The IoT presents several advantages.

Some of the benefits are mainly for particular industries, while others apply to several types of industries (Paruchuri, 2018). We would look into the following IoT advantages to business enterprises.

- IoT monitors the process of the business.
- It makes the customer experience (CX) more efficient.
- IoT through automated processes helps save time and reduce cost.
- IoT through the connected network of data helps improve employees' output.
- It also connects various business models
- Through data sharing allows businesses to make better decisions.
- In saving time and cost helps improve revenue.

The connected network system of the IoT allows companies to select a proper technique to use for their business as it gives them the information and tools for better choice. IoT uses sensors and other devices to manufacture, transport data. Through machine learning, IoT manages infrastructure within the organization making these industries more digitalized and transformed.

For instance, IoT can help improve farming and make it easier to farm in the agricultural industry. Information and data about the weather can be collected by sensors connected to the Internet of Things which detect rainfall, temperature, and the content of the soil, along with other pieces of information that may help improve the industry (Vadlamudi, 2017). IoT through automated machines would help improve farming methods. Also, the need to manage the operations of machines, pieces of equipment, and infrastructure can be so solved using IoT.

For instance, structures and buildings could be monitored by sensors that can detect changes in events and malfunctioning of infrastructures and equipment within the industries. These management techniques are cost-effective, save time, and increases the quality of workflow.

Also, IoT can be used to automate electrical systems by manipulating and monitoring systems in a home. Also, people can be monitored by IoT in an intelligent City to limit unnecessary cost and energy use (Vadlamudi, 2018). The business, Heath, financial, and manufacturing industries can all be influenced by IoT.

Some of the downsides of IoT are:

- The risk of data and information theft by hackers. The growth of IoT means an increase in the connection of devices and the growth of data sharing between connected devices. The impact and likely hood of a hack would also be huge.
- The volume of data used would also increase. This would make it a more complicated task to manage the large inflow of data in IoT by persons and content management systems.
- Through the shared network, whenever a bug affects a system, there is the tendency that it may also affect all the devices connected and corrupt them.
- IoT lacks an international standard for the compatibility of the device. Issues may come up due to the difference of the manufacturing devices to communicate with each other.

Standards and frameworks for IoT

Multiple standards for IoT have emerged; a few of them includes:

- IPv6 over Low-power wireless personal Area networks: this is shortened as 6LoWPAN. This standard is characterized by the Internet Engineering Task Force (IETF). This standard allows for communication by low-power radio. Devices supported by this standard maybe be 804.15, Home Automated machines like Z-Wave, and Bluetooth Low Energy.

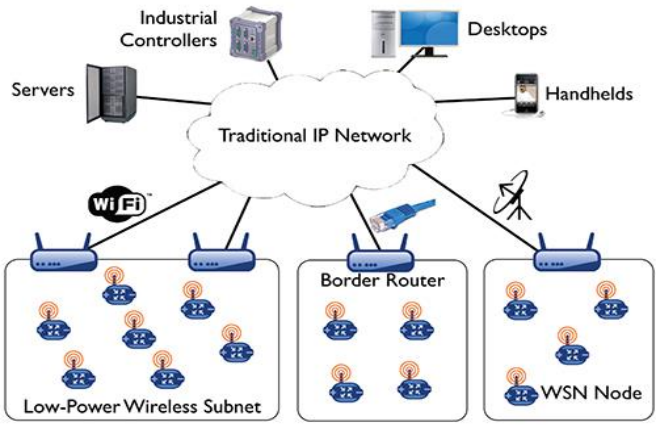

Figure 2: 6LoWPAN (Source: designworldonline.com)

- ZigBee IoT network system is efficient. Low power and low data rate consumption. It is utilized by large corporations. The standard is based on the IEEE 802.15.4 standard. Intelligent devices can work on several networks and speak and understand each other using Dotdot. Dotdot is a universal script that empowers secure devices.

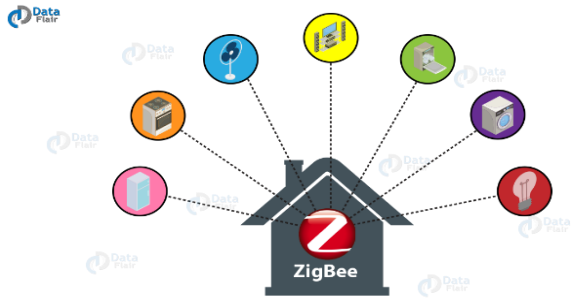

Figure 3: ZigBee IoT (Source: data-flair.training)

- LiteOS: this is an operating system that is similar to UNIX OS. LiteOs functions as a platform for intelligent devices to develop (Paruchuri, 2017). It supports web-enabled devices such as smartphones, applications, and the internet of vehicles (IoV).
- OneM2M: this was invented by a global standardization body to allow IoT applications on the network to interact by a reusable standard. To connect hardware and software to devices, service layers are embedded. These service layers are for a machine to machine communication.
- Data Distribution Service (DDS): This standard was invented by the Object Management Group (OMG). It enables real-time and advanced machine-to-machine interaction. It makes the IoT easy to use.
- Advanced Message Queuing Protocol (AMQP): This allows for advanced messaging using embedded programs and messaging applications between organizations and devices. It is an open-source standard for non-synchronized messaging by wire. The protocol allows client-server message sharing and IoT device management.

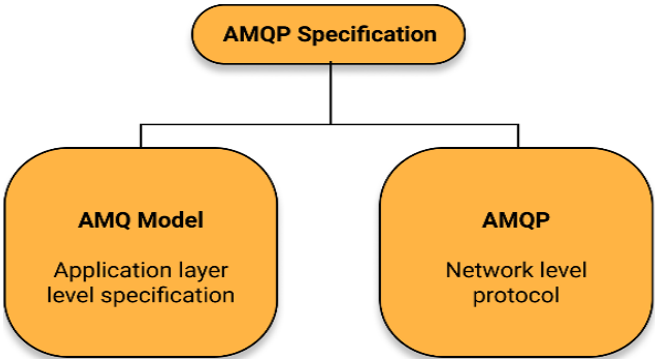

Figure 4: AMQP (Source: www.cloudamqp.com)

- Constrained Application Protocol (CoAP): This protocol was created by IETF. It indicates the way low-power and limited computer systems may perform in the IoT.
- Long Range Wide Area Network (LoRaWAN): This protocol is for wide area networks. It enables networks with large capacities such as big industries with structures or smart cities with thousands of low-power systems.

Private and Security Issues of IoT

IoT applications cut across many technologies and advanced internet worlds, ranging from consumer to industrial sector. Smart homes with smoke detectors, Artificial Intelligence security systems, and connected devices can be controlled through computers or smartphones (Vadlamudi, 2016).

Through the IoT, billions of devices are brought into the system, establishing a connection in the internet and IoT network. It brings about the need to use even more data and a bigger database. The data and data have to be kept secured from possible hack or attacks. The growing database of devices on the IoT has been a cause of fear and concern the security and privacy of data remains a big issue.

A popular IoT threat was in 2016. The Mirai attack used the botnet to bypass Dyn. Dyn provides hosting and servers for domain names and websites. The hack affected a lot of websites for a long time. Many view it as the longest distributed denial-of-service (DDoS) hacks ever witnessed. The hackers used poorly secured devices on the IoT network to gain access to the network. As mentioned before, the interconnected nature of the IoT network makes it easier to attack the system. A weak device on the network could expose the whole network and database to possible threats. A hacker needs to use a vulnerable device, manipulate the data, and gain access to make it useless.

Regular updates help prevent security breaches. Most manufacturers don't update their products on time. This makes it easier to hack the device. Devices on the network from time to time usually request for personal data of users. This could include their biodata, addresses, bank account details, and so on. This data becomes a target for hackers. Privacy on the IoT is another factor and cause of significant concern of users. Companies that produce IoT devices can use them to gather personal data and sell them too.

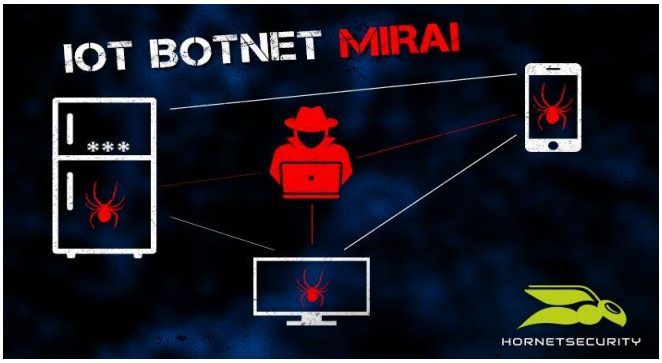

Figure 5: IoT Botnet Mirai (Source: hornetsecurity.com)

WATERMARK SIGNATURES

A watermark is an embedded signature or signal on/in a thing. It could on a video, image, or other types of files. The signature maybe is inaudible signals in a video or a unique encrypted key on an image. Watermarks are unique, and they help trace the owner of a copyrighted property using the unique identifier. Data are hidden in properties digitally and sometimes contain data that connects back to the owner or original Carrier signal. To check the originality and integrity of the thing or detect its actual owner, digital watermarks are employed for verification. Watermarks are employed to trace infringement on copyright and currency checks.

Watermarks help in:

- Tracing assets of persons
- Identification of the creator or registered owner of the content.
- Knowing the legitimacy of content. It could check whether the content was gotten legitimately.
- Visible watermarks serves as branding mechanisms.

However, a content management system protects contents using imperceptible watermarks, which may embed signatures or UIDs. Here the content and the watermarks cannot be distinguished, but the watermark remains part of it. A million copies of an image could have UIDs for identification.

Types of Watermarks

- Visible Watermarks –These are watermarks that can be seen with the eyes
- Invisible Watermarks –

The steganography technique hides and embeds messages into things (Vadlamudi, 2015). Invisible watermarks are watermarks that cannot be seen with the eyes; they are encrypted into media using steganography.

Public Watermarks –

These are zero security watermarks. They are open to the public, and anyone can modify them using specific algorithms

Fragile Watermarks –

These are watermarks that can be easily removed by data manipulation. A detecting software program should be in place to detect possible changes to a fragile watermark if these types id to be used.

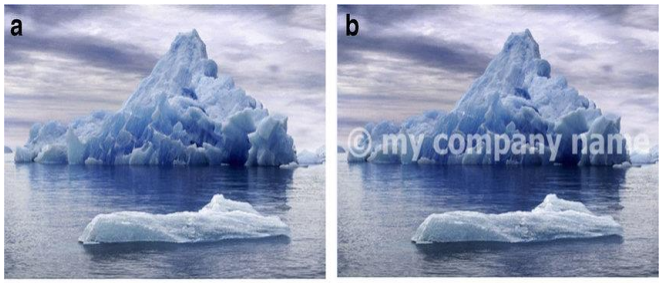

Figure 6: Visible and invisible watermarks (Source; www.researchgate.net/figure/sible-and-invisible-watermark)

WATERMARKING APPLICATIONS CONTENT CONTROL

One of the main issues solved by watermarking is ability to track leaked classified information, proprietary corporate research, or unauthorized copies of movies. Companies can monitor videos and records that are sensitive or classified. Digital watermarks can trace someone who leaks confidential information and help keep track of the distribution of sensitive material. An example is the use of watermarks in studios to track whoever has unauthorized access to work prints and dailies that have not been released. This implies that whoever makes and disperses illicit duplicates can be followed. Piracy is a huge issue of worry for advanced film. Whenever shipped to off cinemas in amazing advanced structure, Films could be replicated effortlessly and conveyed wrongfully. Thus, advanced watermarks distinguish every individual duplicate, facilitating tracing and controlling copyright infringement.

Content Identification

Inserting or putting watermarks on the content surface can assist content owners distinguish the source of particular content? For instance, broadcasting agencies can tell where the recording was recovered, whether from a staff journalist, a consultant, or an outsider. The distinction may not be spotted simply by reviewing the content, however your watermarking framework can remarkably distinguish every image, file or video. All in all, how do imperceptible watermarks work? All imperceptible watermarking are instances of steganography. Steganography is the act of hiding messages within messages so that the sender and expected beneficiary can know the presence of the message, and all the more critically, figure out how to recover it. No one but the recipient is aware of how to retrieve this secret message.

In a similar way, watermarking makes slight modifications to each image in the video so that no one can tell that there have been alterations. More complex methods of watermarking are in use today. The recipient of the

watermarked image will be left with grey dots on a black background after the original image has been subtracted from the watermarked image. A lot of digital watermarking methods in use today embed codes to modify the image (transcoded, cropped, sealed, etc.) whilst maintaining the ability to extract the watermark. In addition, more recent methods have no need for the original copy for comparison to remove watermark data. Many techniques are similar to those used in compression technologies. The watermark on the final image ends up as slight variations in color. You cannot find the watermark data if you have no knowledge of the mathematical "key."

A watermark is:

- Data added to and frequently covered inside a content
- Data of normally a modest quantity, regularly an extraordinary recognizable proof number
- Difficult to eliminate by picture modification
- Very elusive without information on the mysterious key
- Usually, a similar data rehashed in each video outline

If a watermark is created by one technology, it can't be perused by an alternate technology system. Also, regardless of whether two systems utilize a similar technology, one client won't go through the watermark of the other without the unique key that uncovers both where to discover the watermark and how to interpret it. The fundamental cycle of adding a watermark is very straightforward (Ganapathy, 2017). The watermark is commonly executed as a channel applied to an uncompressed content, which brings about an uncompressed content outline containing the inserted data. The data to be hidden and the "key" that enables the data to be hidden must be programmed with the watermarking filter (Neogy & Paruchuri, 2014). Digital watermarking is typically carried out as a transcoding process since it is usually performed on uncompressed frames. The transcoding process involves:

- DEmultiplexing or demixing of the video by the transcoder
- Decoding it into uncompressed frames
- Feeding the frames through the watermarking filter and
- Compressing the resulting frames and multiplexing or muxing them into the final format(s)

There exist several watermarking strategies that maybe be performed straightforwardly on compressed images, they are frequently confined to keeping up a similar packed configuration. Watermarks can only be useful when they can be extracted and compared existing watermarks.

A few apps give both watermarking technology and tracing services. Furthermore examine content on the web and look for watermarked content, however others give only the technology with the suspicion that solitary the client will implant and spot watermarks. Your necessities and spending will decide the watermarking you do.

Copyright Control

Cross-referencing actual usage rights and permissions in a watermarked database will ease the tracking of both authorized and unauthorized content uses. In order to determine whether a database contains unauthorized content, creators and distributors of content will use watermarks. Also, in order to detect the clips licensed in commercial programming, stock footage providers will use watermarks. Content creators can store all sorts of very vital tracking information associated with the content on metadata. Metadata can be utilized to complement watermarks by putting away significant client data, (for example, the maker of the substance and who adjusted it), history of utilization, explicit working framework which a video has been played on, and by what form of player, data about which networks content has gone on and the limit it went. This data will be of great use during legal examinations to follow pilfering activities, reveal rebels inside the association, etc. One of the first applications that combined metadata with watermarks is the Gracenote's TuneUp Companion for iTunes. Cleaning up metadata associated with recorded music is the app's main use.

Connecting Images on IoT through Watermarks

Images that are utilized across many stages disregard copyright arrangements and remove the credibility of the images (pictures and photos) taken with difficult work by a person. Connecting images through watermark signatures creates and enrolls a unique number which ties up the human and the camera which is getting utilized so that the photograph taken by the individual will leave a unique identifier or mark that will make the image copyrighted and transfers to the cloud for direct utilization on any pages in IoT (Ganapathy, 2016). The immediate income of the copyrighted picture goes to the individual who owns the photograph. This way, the content administration system that produces pages can utilize the images and offer the benefits dependent on income from the guests visiting the page and loving the content.

Images as part of the things connected and exchanged in the Internet of Things would be monitored using their unique keys for signals (Paruchuri, 2015). The unique keys embedded in the images would be associated and connected in the IoT in three different layers.

- Embedding
- Attack
- Detection.

The embedding of the IoT accepts the data and owner of the picture with the unique watermark key. The next process is attack detection. The watermarks are signals and signatures of the image and leave behind traces as transferred from one person to another. An attack happens when a person modifies the image within the IoT. The attack is a copyright protection term, where a person makes changes to the image and tries to adjust the watermark; it is regarded as infringing on the owner's

property. A detection algorithm is applied to an attacked watermark. It checks the presence of a watermark. Using imperceptible watermarks on images, the invisible watermarks are embedded in the photos giving traceable signatures to detect attacks on the picture's copyright.

The signature and signals are concealed in the IoT using the steganography technique. Steganography is a technique used in concealing messages within another message. Here the signature is encoded within the images or other media files. The signatures do not draw attention to themselves but serve as an invisible security mechanism. Steganography helps to conceal the message.

IoT association of images with watermark signatures to pages across content management websites creates a connected database to solve the different issues, such as providing copyright protection of content, effect detection, tracing traitors, and maintaining the originality of related data on IoT. Owners with content will generate and register a unique image signature or key on the IoT. This would connect the human and the camera used to snap the image to have a unique identifier, detector, and signature that will allow for multiple advantages. This connection in the IoT system aims to allow for privacy, income generation, integrity authenticity, non-repudiation, etc.

Some Advantages of Connecting Images on the IoT through Watermarking Content

Copyright protection

Images on the IoT are openly displayed, and web transfer by content management systems on the IoT remains a threat to copyright. It can lead to copyright infringement, such as piracy and misuse. An image could be shared without the consent of the owner. It can also be abused or defaced, causing copyright infringement. Watermarking images for connection in the IoT helps protect images. Invisible signatures and keys would link your image to you for reference, and signals can detect any infringement on your image in the IoT.

Income generation

Watermarking images with unique keys which are traceable to the owner of the image makes income generation possible through licensing. Where images are watermarked with registered keys, they become traceable to registered owners who own the copyright. The use of a watermarked image would require payment for a license. The license allows third-party in the IoT to use the image. This way, the watermarked image(s) in the IoT generates income for the registered owner.

Maintains originality

A watermarked image will maintain the originality of such an image on the IoT. It also makes it possible to trace the registered owner of the picture. The watermark prevents copying of the image as it serves as the copyright protection mechanism in the IoT.

Conclusion

As the world develops, more technological advancements spring up to solve problems. Digital watermark, along with its features, would help curb piracy, copyright infringement and generate income for copyright content owners. Billions of images exist on the internet of things and the open for use by anybody anywhere at any time. The internet of things connects all things using web servers. When embedded into an image, unique identification keys would make it trackable, traceable and it would also authenticate the image. Using a watermark on an image would tie the owner and the camera that took the picture together with its UIDs. Though there are upsides and downsides, IoT association of images across content management websites proves to be a positive idea in the long run.

References

Ganapathy, A. (2016). Speech Emotion Recognition Using Deep Learning Techniques. *ABC Journal of Advanced Research*, *5*(2), 113-122. https://doi.org/10.18034/abcjar.v5i2.550

Ganapathy, A. (2017). Friendly URLs in the CMS and Power of Global Ranking with Crawlers with Added Security. *Engineering International*, *5*(2), 87-96. https://doi.org/10.18034/ei.v5i2.541

Ganapathy, A. (2018). Cascading Cache Layer in Content Management System. *Asian Business Review*, *8*(3), 177-182. https://doi.org/10.18034/abr.v8i3.542

Neogy, T. K., & Paruchuri, H. (2014). Machine Learning as a New Search Engine Interface: An Overview. *Engineering International*, *2*(2), 103-112. https://doi.org/10.18034/ei.v2i2.539

Paruchuri, H. (2015). Application of Artificial Neural Network to ANPR: An Overview. *ABC Journal of Advanced Research*, *4*(2), 143-152. https://doi.org/10.18034/abcjar.v4i2.549

Paruchuri, H. (2017). Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review. *ABC Journal of Advanced Research*, *6*(2), 113-120. https://doi.org/10.18034/abcjar.v6i2.547

Paruchuri, H. (2018). AI Health Check Monitoring and Managing Content Up and Data in CMS World. *Malaysian Journal of Medical and Biological Research*, *5*(2), 141-146. https://doi.org/10.18034/mjmbr.v5i2.554

Vadlamudi, S. (2015). Enabling Trustworthiness in Artificial Intelligence - A Detailed Discussion. *Engineering International*, *3*(2), 105-114. https://doi.org/10.18034/ei.v3i2.519

Vadlamudi, S. (2016). What Impact does Internet of Things have on Project Management in Project based Firms?. *Asian Business Review*, *6*(3), 179-186. https://doi.org/10.18034/abr.v6i3.520

Vadlamudi, S. (2017). Stock Market Prediction using Machine Learning: A Systematic Literature Review. *American Journal of Trade and Policy*, *4*(3), 123-128. https://doi.org/10.18034/ajtp.v4i3.521

Vadlamudi, S. (2018). Agri-Food System and Artificial Intelligence: Reconsidering Imperishability. *Asian Journal of Applied Science and Engineering*, *7*(1), 33-42. Retrieved from https://journals.abc.us.org/index.php/ajase/article/view/1192

--0--