Wireless Sensor Networks, Internet of Things, and Their Challenges

Chijioke Worlu, Azrul Amri Jamal, Nor Aida Mahiddin

Abstract— ***Internet of Things (IoT) is currently one of the top technological concepts where users and objects are interconnected using wired and wireless technologies such as Wireless Sensor Networks (WSNs), ZigBee, NFC, RFID, GPRS, LTE and Bluetooth, anywhere and anyplace. Within the past ten years, the idea of IoT has drawn massive consideration from both the business and research communities. Application domains may have many substantial benefits by means of an IoT approach. The idea of this field of study is to portray a basic knowledge of smart environmental monitoring system based on IoT. It has been stated in various studies in the past that IoT is facing multiple issues such as authentication, identification, availability, security and privacy, and socio-technical trust system (STTS). Nowadays, existing smart environments are continuing to face major IoT setbacks and challenges with regards to security, privacy, and STTS. Creating a STTS comparison in IoT is one of the principal significant breakthroughs necessary for building stable structures which will serve to eliminate doubt and technical setbacks. This study will present an outline of security, privacy and STTS in IoT while using a simulation method for comparing the results and justifying the outcomes. It aims to highlight and define the effectiveness of trust-management and how it should be exploited in IoT. The results will be indicated based upon past and present study result comparisons.***

Index Terms: Challenges, IoT, security and privacy, smart environment monitoring system, STTS, WSNs.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is defined as a small scale gathering nodes of a sensor used for monitoring, sense, capturing and processing the data around an application— i.e., phenomena of focus [1]. As a result, these nodes are resource-needy and at the same time extremely dependent on battery control, storage, computation, data size and accessible bandwidth. Normally, these nodes are fixed in a particular way and also left as a single node in a remote and human-inaccessible point to execute tracking and recording of information. The word "wireless" has turned into a nonspecific and widely inclusive word used to portray communications in which electromagnetic waves are utilised to send an indication over part or the whole communication pathway [2].

The terms “Internet of Things” represents mostly wide innovation and research that empowers Internet users to connect into the universe of physical items [3]. Nevertheless, there are however two fundamental understandings of what IoT implies, and in this way, what sort of technological innovations should be considered. Alternatively, IoT is regularly connected with technologies—for example, Radio Frequency Identification (RFID), low range wireless communications, real-time localisation and network sensors. From this point of view, the primary factor of IoT is characterised by the utilisation of ubiquitous sensor communications and allows devices functionality. Then again, there is a particular research line suggesting that the significance of the word "thing" should not be limited to a physical thing, but rather involves theoretical and virtual segments, specifically those of service. From this standpoint, this current work endeavours to advance from this gap, and will attempt to consolidate such differentiating services [4].

The principal goal of this current study is to present comparative information based on IoT smart environment monitoring systems. The proposed simulation methodology of the current study is henceforth intended to deal with extensive accuracy measures of information originating from security, privacy, and STTS aspects, as well as those included by standard IoT issues and situations.

II. LITERATURE REVIEW OF WSN

WSNs provide indispensable advantages over traditional methodologies for a variety of applications including environmental monitoring, smart homes, human services and national security. WSNs are a component of the Internet Protocol (IP) that formulates the IoT by connecting objects of everyday life to the Internet [5].

Based on detection scope innovation mainstream has tremendously improved, while WSN devices have become relatively more cost-efficient. However, this has shown a blueprint to a huge growing tracking extension of the sensor-equipped system condition, structures, vehicles and devices. The primary components of wireless networks revolve around the current advances in the innovation of networking technology; for example, wireless communications and mobile ad-hoc networking in combination with device-coordinating technologies. Hence, WSNs is situated to be utilised in monitoring transport infrastructures for example rapid-transit tracking, bed tracking, equipment tracking, and bridges as well as in tracking vehicle whereabouts and safety specifically wheels, wagons, bogies and chassis. Condition-monitoring limits the need for human examination requirements through automated monitoring, reduces repairs by identifying problems before they occur, and overall improves well-being and reliability standards [6], [7].

Revised Manuscript Received on September 14, 2019.

Worlu Chijioke, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, UniSZA, Terengganu, Malaysia.

Azrul Amri Jamal, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, UniSZA, Terengganu, Malaysia.

Nor Aida Mahiddin, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, UniSZA, Terengganu, Malaysia.

Retrieval Number: L110210812S219/2019©BEIESP
DOI: 10.35940/ijitee.L1102.10812S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Previous research by [8] led to the development of a WSN-based monitoring system in support of farmers decisions with regards to pesticide application and quantity regulations; and based accordingly on the real and relevant needs of agricultural crops. The study indicates that in recent years, wireless innovations have gain the momentum to a degree incorporated into the industrial accuracy of greenhouse domain. Due to the inconsistency of crops, a recognised degree dimension and fleeting comminute is required to give significant ecological measurement parameters. WSN primarily manages connected technology due to the scalability, reasonable price, universality, and self-organisation of smart nodes. The possibilities for fine-grained monitoring and activation have unfortunately been misused. Nevertheless, in improving administrative regulating of irrigation, manure and pesticide controls, a substantial economical privilege and more cost-effective reproduction is recommended.

A. Differences between WSNs and IoT

The interconnectedness between humans and devices has completely informed the approach of this new paradigm shift known as the IoT. IoT implants intelligence and technical knowledge into our environments by transforming accumulated data into smart data. As such, WSN is considered a basic factor of IoT [9]. WSNs provide us with the information used by the IoT. They are typically in control for monitoring and keeping track of the physical or climate status, and for linking the gathered information to a centralised position [10], [11]. This means that WSNs are a collector and provider of data, while the IoT is the central location that intelligently analyses the data gathered using the Internet and presents the information for human accessibility.

B. WSNs Technology and Applications

Wireless technology can be prepared to achieve all targets on the surface of the earth. Because of the huge achievement of wireless voice and informing communication service, it is really remarkable that wireless communication is starting to be connected to the space of individual and people who deal with business. A particular positions technology of settling the plan of the tower in China has been proposed, technologically advanced a remote monitoring system for vibration of intersection and spreading over digression tower, acknowledged on-line testing of the vibration condition of transmission tower, remote transmission through wireless system, constant examination of vibration and modal change and vibration reaction of sudden loads of transmission tower under complex environment, which establishes a framework for assessing the safety status of transmission tower [2].

Hence, in [2] produced an application that concentrates on monitoring the health of cows, gathers and examines information acquired from sensors mounted on dairy cattle. The proposed system controls the sensors wirelessly with a microcontroller and utilisations GPS to control cows' development.

Furthermore, in [12] creates a virtual wall application that can control the creature's (animals) movements and space without man-made perpetual structures. The dairy animals are furnished with a shrewd neckline comprising of a GPS unit and a sound intensifier. Therefore, a previous study indicates that in some case, ecological monitoring is additionally subject of research.

C. Classification of WSNs

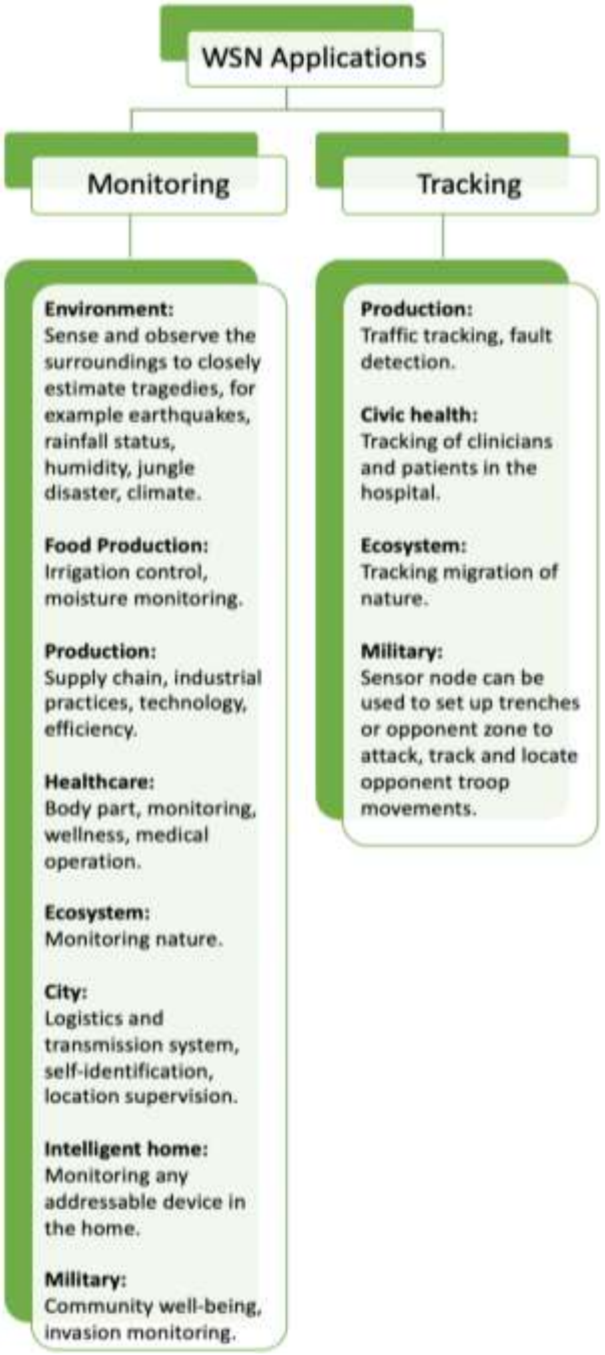

WSN Applications
Monitoring
Tracking
Environment:
Sense and observe the surroundings to closely estimate tragedies, for example earthquakes, rainfall status, humidity, jungle disaster, climate.
Food Production:
Irrigation control, moisture monitoring.
Production:
Supply chain, industrial practices, technology, efficiency.
Healthcare:
Body part, monitoring, wellness, medical operation.
Ecosystem:
Monitoring nature.
City:
Logistics and transmission system, self-identification, location supervision.
Intelligent home:
Monitoring any addressable device in the home.
Military:
Community well-being, invasion monitoring.
Production:
Traffic tracking, fault detection.
Civic health:
Tracking of clinicians and patients in the hospital.
Ecosystem:
Tracking migration of nature.
Military:
Sensor node can be used to set up trenches or opponent zone to attack, track and locate opponent troop movements.

Fig. 1: A reproduced classification of WSN application adapted from [13]

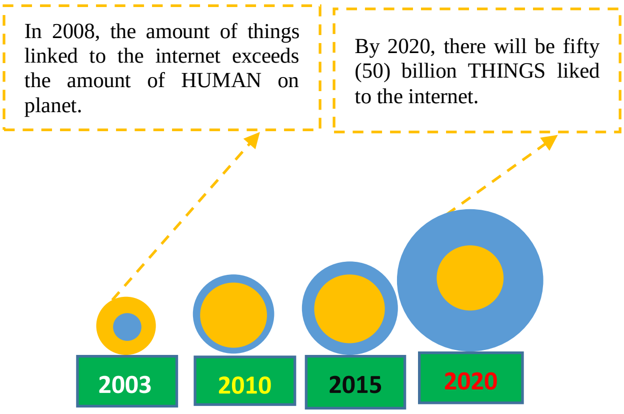
A study by [13] indicates that WSNs applications has many real practical advancement technologies that has been turned out for years. For that reason, applications for WSNs is mainly classified into two categories known as monitoring and tracking. The part of WSNs utilisation that supervise, analyse and prudently monitors the movement of a system real time is identified as the monitoring part. While the part that track an overall utilisation for succeeding the modification of an event, a person, an animal etc. is identified as the tracking part.

Another study has mentioned that obtainable monitoring applications includes inside and outside ecological monitoring [14], industrial monitoring [15], precision agriculture [16], biomedical or health monitoring [17], electrical network monitoring [18], military location monitoring [19], etc. more classification ware summarised in Fig. 4 in their study.

III. LITERATURE REVIEW OF IOT & RESULTS

The previous study by [20], claimed that The Origin of IoT, was first introduced in 1999 by Auto-ID Center. They further claimed that Auto-ID Center has turned into a positive spotlight in the United State to empower and encourage the development of IoT, and the approving it as a future strategic recently-emerged industry.

The European Commission anticipates that between fifty (50) to hundred (100) billion apparatus will be linked to the cyberspace by the year 2020 [21].



In 2008, the amount of things linked to the internet exceeds the amount of HUMAN on planet.

By 2020, there will be fifty (50) billion THINGS liked to the internet.

Fig. 2: A reproduced growth model of objects that is related to the web adapted from [22]

As shown in Fig. 2, the number of things connected to the Internet in 2008 has exceeded the number of people on Earth. By definition and in a perfect world, the connection accessibility of individuals, objects within, everyone, anything and anywhere is triggered by IoT and is utilised within any given organisation or administration [23]. As evidenced by the rapid growth in monitoring technologies, the primary definition of IoT is not by application or the client needs, but rather by the mechanical advancement.

A. IoT

IoT is known as a versatile areas of trending innovation. The idea of IoT is gaining more considerable attraction on the areas of extensive range of industries. For business firms, the real significant innovation of IoT is broadly recognised when associated mechanisms has the ability to interact with each and has the strong connectivity to combine with trader checklist schemes, client aid schemes, corporate brainpower supplication and corporate logic [24]. Moreover, for most important reasons for worthy IoT works in the real world that has been indicated above, this current investigation has prompted to focus on the improvement of IoT based on the ecological smart monitoring system. The fundamental attributes of IoT executions are the transmission of modules, for example, sensors, IoT hubs and electronic devices within various communications way out distributed nationwide. The synchronisation of the modules and controls is another test and challenge for IoT approaches and relies upon parameters such as dormancy, jitter and control protocols [25]. IoT includes numerous developments such as architecture, sensor/identification, coding, transmission, data processing, networking, and discovery. The development of IoT does not solely depend on the advancement and standardisation of technology, it also depends on the change of our social perception and judgment, knowledge, rules and laws. For instance, in the future IoT era, the way we live like mechanisms or nodes of the network and the exposition (the way we live our lives) of our activities to the general societies may deliver numerous serious security and privacy (protection issues). The standard, reliability, and durability are additionally key uncertainties for IoT development [20].

Careful consideration must be given to the fact that there are several aspects and definitions of IoT, depending on the frame of reference. When bearing in mind that the services offered useful IoT objects that represents "a world where things are automatically accessible and can directly communicate to PCs and [to] mankind" [20], from a connectivity standpoint, IoT signifies that at any time, in any place and for anyone, "we will now have a network for anything" [21]. From a communications viewpoint, IoT indicates "an overall network of interconnected objects that are unique tools based on addressing them" [26], [27]. And from a networking standpoint, IoT is the Web itself—having been developed "from a network of interconnected things to a network of interconnected PCs" [28].

According to a study by [29], IoT application has a wide coverage that must be systemised in a comprehensive and applicable way so as to meet the specific needs of today. The essential methods of classifications in IoT applications are presented and abridged below in Table 2. IoT works in serving entirely different user demographics-including individuals, companies, and society at large. Additionally, it covers a wide scale of application domains [30]-[32]. For example, smart homes and environments, smart manufacturing, smart cities and energy production, green agriculture, logistics, healthcare as well as media and future applications, to mention but a few.

B. Application Classification of IoT

Table 1: Application classification—Summary [29]

Criteria for Classification	IoT Classes
Domain [30]-[32]	(1) Transportation and logistics (2) Healthcare (3) Environment (4) Personal and social (5) Futuristic application (6) Food/water (1) Transportation and logistics (5) Futuristic applications (6) Food/water monitoring (7) Living (8) Manufacturing (9) Energy (10) Building (11) Industry (12) City (13) Security and safety (14) Communication (15) e-society (16) Vehicular (17) Sport and leisure
Flexibility and amount of distribution [33]	(1) Secured and concerted (2) Secured and detached (3) Mobile and concerted (4) Mobile and dispersed
Retard of tolerance [34]	(1) Flexible (2) Inflexible real-time (3) Retard-variable (4) Rate-variable
Reporting of data mode [35], [29]	(1) Date and Time-process (2) Query-process (3) Event-process (4) Progressive-based (5) Hybrid-process
Dependable, obtainable and end-to-end latency [36]	(1) Monitoring-based and critical task (2) Monitoring-based and non-mission critical (3) Control-oriented and critical task (4) Oriented-guide and non-critical task
Characteristics and requirements [32]	mMTC and uMTC

The notion of a general IoT necessitates various classifications to be combined into a primary and integrated area. It deals in the management of the supporting technologies required in such areas, while taking into account third measurement components such as security, privacy, trust and safety. It is important to note that recent classification criterions and classes of IoT applications are unable to distinguish between IoT domains and the application of IoT. IoT fields are normally considered to be an unambiguous part of IoT applications which assist some massive range of applications through manufacturing affecting companies and consumers. Consequently, IoT fields intersect within the existing IoT classifications with IoT applications [37].

C. Smart Environment Monitoring System

The smart environmental system monitoring is respected as a forerunner in IoT control and monitoring system, however, some of the main significant suggestions of SEMS are known as property and family security, as well as saving of energy. The Control of Networks (CN) and Verizon Home Monitoring (VHM) is clearly important for properties and families, for example, utilisation of internet communication innovation specifically made for home remote control application. Hence, IoT enabled home apparatus for easy communication and gives access to device to monitor and control things remotely via all kinds of devices outside the apartment of the user. The VHM and CN is needed for managing security systems, adjust lighting, and receive programmed event warning, climate control and even bolting and opening entrance [18].

In addition, smart environments are gradually being developed for environmental, health, industrial, construction, military and transportation applications. Such environments typically rely on smart apparatus that collect information from the technological world, then subsequently handling and assuring that data that comes from data processing centres-creating, information-based services are occasionally delivering as a few environmental events [18].

D. Sensor Networks

Network sensors could be listed as one of the major advancement in empowering IoT [32]. This technology can structure the glob by building a recent IoT trend and providing the accessibility to estimate, induce and the environmental impacts [33]. An up to date advances technological upgrades have given devices high productivity and facilitated the large-scale use of remote sensing applications [34]. In addition, smartphones are connected to a decent range of sensors and thus enable an array of mobile applications in a number of different IoT regions. To this end, the main assignment of testing is to process the sensor's extensive information on vitality, system limits and vulnerabilities [41].

E. Sensor Node Design

Sensor plays a major role in application of IoT. There is a mandatory need of sensor nodes for IoT application that made their details essential for application execution. Thus, rapidly spreading in-situ fire detection has been chosen as the reference point for ecological WSN design. In [42] further mentions that one of the greatest vital necessities is reducing sensor node costs. Similar to the low costs of applications, sensor nodes appear to be in a position to sustain a lengthy maintenance-free checking time, as well as capable of supporting a straightforward and reliable distribution strategy. In [42] claimed that physical size and weight are equally important, particularly in the way that they are transported for backpack distribution. Further claims are made about node energy sources affecting many of its features. Batteries can provide a consistent flow of efficiency, on the other hand, has a time restriction and may require an expensive replacement maintenance process.

F. Location and Sensors in IoT

A past study by [37] has stated that all IoT things are at a location. Location is a key piece of information for the vast majority of the new and inventive applications empowered by IoT. Location information is universal but not constantly accurate. Location data quality can be easy to uphold, however slight mistakes can occur sometimes and cause disappointments, harm and loss. The study claimed that accurate handling of IoT location data is being identified as the standards for a location well recognised by several standards developing an organisation, specifically as set up by the Open Geospatial Consortium (OGC). Sensors and actuators related to IoT devices are bringing another mindfulness and control of the environments in which we live and work.

G. IoT Architecture

An IoT architecture fundamentally consists of the arrangement of low-handling identifying components known as nodes and a layer of cloud-based which qualifies the client to track these continuously and remotely. In addition, in [43] introduced an advanced IoT method to send a network wireless sensor connected to the natural temperature and relative humidity monitoring system to the healthcare and clinical labs. Such facilities also handle medicines and organic cases which require routine monitoring. Accordingly, the healthcare sector has become the main unique pioneering industrialised in terms of recognizing and emerging the potentiality behind the distribution of connected services (eHealth) since the IoT paradigm first began attracting attention.

H. IoT Architecture Illustration

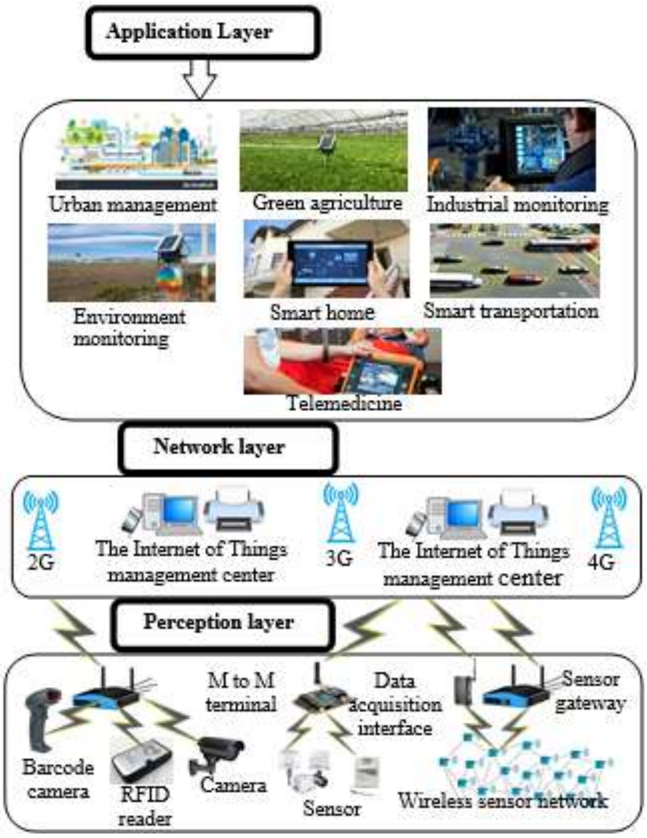


Fig. 3: A reproduced architecture of IoT model adapted from [44]

This current study adapted the previous study architecture model to investigate the problem of the current study and achieve its objectives. Based on the previous study by [44], the architecture model of IoT is outlined and indicated in their study in Fig. 1 and 3 in the current study. In [45] states that the most basic architectural model of IoT consists of the following three layers: (1) application layer, (2) network layer and (3) perception layer. Moving on, data-obtaining interface outlines are mostly connected to an extraneous layer within the IoT known as the recognition layer [40]. This layer is essentially composed of sensors, RFID readers, cameras, M2Ms and various data gathering terminals [46]. The data security interface is accountable for integrating and collaborating on the various environments, in addition to collecting sensor data.

I. Essential IoT Technology

Successful IoT deployment products and services that widely utilise IoT technology:

a) RFIDs;
b) WSNs;
c) IoT application software;

d) Middleware; and
e) Cloud computing

J. IoT Technology and Applications

IoT development speedily assist the IoT application that focused on the heap industry and specific users, while networks and devices allow connectivity of physical things. IoT application gives reliable vital device-to-human and device-to-device communication. IoT device applications need to ensure that information is received and properly acted according to a suitable specific way, a simple example is that of logistic application monitoring that has the transported status of goods such as organic products, fresh products, meat and dairy terms. Furthermore, during logistics, quality control of climate change, shock and humidity is regularly monitored and suitable movements are strategically and naturally made to preserve goods spoilage from a long distance when connection is out of courage [47].

According to [47] claimed that "some examples of IoT applications in existence can be found in Smart Environment, Smart Greenhouse, Smart Cities, Smart Water, Smart Metering, Security and Emergency, Industrial Control, Home Automation and Electronic Health". 'IoT' is therefore stationed on devices that can examine sensed data and then transmit it to the user.

K. IoT Challenges

As stated in a previous study by [48], there are some challenges that IoT design would face in the coming future generation. All the devices, nodes connected in associate in nursing IoT design needs to have terribly low latency over reliable links. Because of the vast variety of IoT devices and the use of various frequency bands, there would be a crisis in spectrum house. Although IoT devices are expanding on a daily basis that consumes terribly lesser power, still there'll be a big quantity of greenhouse gas emission because of all of these devices. Finally, IoT architecture not solely must be price effective however additionally they have to be capable of supporting heterogeneous applications and devices [49].

As stated above on IoT challenges, IoT applications will have some more basic needs to tackle, for example, Device addressing, Security, Scalability, Mobility, Anchor-less sending and so on [50], [52]. As mentioned, IoT applications contains numerous heterogeneous devices, and however, content security is a key concern that plays a great roles [53].

A previous study has indicated the challenges of both IoT and ICN in their past study, this past study endeavours to combine them where IoT illustrate the different challenges and on the other hand, ICN illustrates the positive solutions. Nonetheless, their study explained initially how different ICN features can address IoT issues and after that, some use cases and contextual investigations are examined [54].

L. IoT Challenges vs. ICN Future

Table 2: IoT challenges vs. ICN features [54]

No.	IoT Challenges	Information Centric Networks (ICN)
1	Identifying and Addressing	Specifying and Label Resolution
2	Mobility	Mobility, Multi-cast, Multi-homing
3	Security and Privacy	Identifying, Position independence, Receiver-Driven, Content-based Security
4	Heterogeneity and Interoperability	Identifying and Specifying Resolution
5	Scalability	Specifying, In-Network Caching, Content-based Security
6	Energy Efficiency	In-Network Caching, Identification

M. IoT Development Challenges

A study by [38] examines the many IoT developmental challenges facing companies of today. In [38] further states that the presentation of IoT lead to various objections, additionally, there are many businesses with each new problematic advancement of challenges that need investigation. For instance, the blast of information achieved by IoT apparatuses, data centres are faced with major issues in security, privacy, information management, storage monitoring, server innovation and general data centre operations. On the other hand, in [38] claimed that the IoT is a strategic technology paving the way for the industrial production systems of the next generation. The study further states that there are a lot of current issues arising on IoT that are to be considered for further researches.

As mentioned by [55], the present IoT frameworks are not adequately upgraded to satisfy the desirable practical necessities and bear security and privacy dangers. Especially, attacks on digital physical frameworks may cause physical harm and demoralise human life. The ubiquity of IoT devices may prompt a straightforward society through consistent supervision of employees and customers. The study suggested that further studies are required to create and configuration proper IoT security components, including novel disengagement primitives that are strong to run-time attacks, negligible trust handles for digital physical frameworks, and adaptable security protocols.

An investigation conducted by [56], [57] indicates that privacy is one of the primary issues to be considered in IoT. As additional IoT-enabled apparatus and systems are designed, better data privacy problem and objections will inevitably arise—particularly with Big Data Analytics and technological innovation placed to find significance in such data.

N. STTS

Is a system that targets to provide equal balance to social and technical issues when the network structures are been designed. Implementing a STTS technique to the IoT portrays a strong understanding on how the IoT will evolve and stabilise in a smart environment [58].

According to past study by [59] has shown that STTS are another major problem in IoT, which have often been criticised for not definitively distinguishing between social and non-social artefacts. As a consequence, the analysis of the interaction between technological artefacts and social entities is not always clear. This weakness can be both a challenge and an opportunity for human beings and technology to grow into two highly interconnected components within IoT.

O. Privacy Challenges

As mentioned by [38], similar to cases involving smart apparatus and intelligent automotive crisis facilities, IoT apparatus can obtain an enormous degree of information on the area and developments of its users, their health conditions and their personal preferences—all leading to critical privacy concerns. Continued assurance of the protection of user privacy is a must for service suppliers in this situation since the produced IoT information is critical in and liable to enhance the nature of individual’s existence and to reduce service provider's expenses via streamlined activities. As indicated by the 2014 TRUSTe IoT Privacy Index, only 22 percent of cyberspace consumers moved the motion that the compensation of intelligent apparatus exceeded any burden or distresses of theirs regarding privacy. Although the integration of IoT into daily life is picking up steam through intelligent home-based systems and wearable apparatus, recognition and self-confident in IoT will depend primarily on the privacy assurances of its consumers.

P. Security Challenges

As the development of the number and collection of associated devices in IoT networks increase, so too does the potential security risks. Although IoT works to improve our everyday lives as well as the profitability of organisations, it also increases potential physical attack surfaces for programmers and other digital lawbreakers. An ongoing report by Hewlett Packard [60] uncovered seventy percent (70%) of the most generally utilised IoT apparatus accommodating genuine openness. However, these IoT devices usually has no service strategies of encrypting data.

Some IoT applications strengthen solid infrastructures and essential services, for instance intelligent networks and equipment security. On the other hand, other applications based on IoT progressively create large measurements of an individual's family, health and monetary information, which data mining initiatives may attempt to use for their organisations. The perceived lack of security and privacy will likely deter companies and individuals from selecting the IoT as a viable choice. These security challenges might be solved by preparing engineers to integrate additional security arrangements (e.g. interruption avoidance systems and firewalls), as well as by encouraging users to implement these IoT securities included with their devices [24].

Q. Trust

The idea of trust is utilised in an extensive number of various situations and with different significances. Trust is a difficult and confusing idea about which no promise exists in the computer (PC) and information science works, despite the fact that its significance has been generally perceived. Diverse definitions are conceivable relying upon the embraced point of view [4]. A primary complication with several techniques towards classification of trust shows that it has lack of attention in supporting of quantities and method evaluation. A generally utilised definition is the one given by [61] which refers to security methods controlling entrance to resources and qualification that are required to achieve such approaches.

R. Previous Study Simulation Comparisons and Results

In [62] introduced a technique for simulating and modelling attacks with performance examination (which included nodular software execution times and estimations of power consumption). Notwithstanding, their study claimed that the information used in smart environments is provided particularly by WSN, which normally monitor and record physical or ecological conditions and communicate this collected information to some significant spot. Their study adds that some of the most widely known network stimulators are NS-2 (The Network Simulator), NS-3, Cooja, Castalia, OMNET++, GloMoSim, TOSSIM and Avrora. OMNET++, NS-2 and NS-3 are all discrete event network simulation applications. NS-2 provides support for transmission control protocol (TCP) simulations, as well as routing and multicast protocols over wired and/or wireless networks. Their study also highlights an NS-2 open source system for the simulation of the undersea sensor network known as SUNSET. It further states that the testing of protocols and distributed algorithms in genuine wireless channels and radio models, as well as of node behaviour, can be performed by OMNET++, especially those in possession of radio access.

S. Characteristics Comparison of Simulation Developed in Past Study

Table 3: Survey of simulators [62]

Simulation	Traffic Generation	Real SW Code Support	HW Platform	OS Support	Power Consumption	Security Measure	Limitation
NS-2 (Then Network Simulator)	Traffic patterns	×	×	×	✓	×	No real traffic
NS-3	Traffic Patterns	×	×	×	✓	×	No real traffic
TOSSIM	Statically or Dynamically	Only TinyOS	×	TinyOS	With Power TOSSIM	×	Only for TinyOS code
UWSim	Dynamically Under	×	✓	×	×	×	Only for Water networks
Avrora	Real	✓	Limited	×	✓	×	Only for Mica2 Sensor nodes
Castalia	Real	✓	×	×	✓	×	Not a sensor specific platform

In [63], the author mentioned that both simulation results (Tmote Sky platform) and hardware testbed results, via the OpenMote platform, were presented. This permits real-word test bed results to be achieved and verified in combination with simulation-based measurements. They further highlight that, to better comprehend the protocol used in the study, it is important to present different metrics. This investigation shows the constancy and dependability of the system, as simulations alone are unable to capture the dynamics and complications of the present reality. The displayed system gives a few highlights that are helpful in reality executions of WSN in healthcare industries. For instance, low-energy utilisation, high accuracy, confidentiality, integrity, and accessibility. These are significant as they encourage hazard evaluation and supervision of the system, in addition to being responsible for data security. In [63] claimed that the simulation outcomes of their study were closely matched with the ones from the real-world deployment. However, it includes identifying the correct malicious node ID(s), false positives or negatives, and the formation of a new routing path [63]. In [64] mentioned that the simulation result found in their study was promising for the expected utilisation. The study further states that it encourages new clients to effectively start up a simulation and is extremely valuable amid development and test stages. It underpins heterogeneous networks, concerning both simulation hardware and software. It is stated in their study that large-scale conduct protocols and algorithms can be seen by utilizing the fundamental set of plugins or by effectively broadening them.

Moving on, in [65] stated that the outcomes discussed in their study are measured after approximation of 95 simulations and the protocols discussed indicated to be energy productive with cluster topology. Moreover, their study explains that with broad simulations on randomly positioned sensor nodes, the proposed strategy is approved in judgment with the old-style WSN ideas and observed to be more preferred and supported for different uses of IoT. Their study claimed that the simulation outcomes demonstrate that the new plan is more energy effective and adaptable than conventional WSN ideas and therefore it can be actualised for proficient communication in the IoT.

In [9] indicate that the results found in their study proved to be extremely significant in choosing a method to the destination based on the proposed algorithm. This is through utilisation of a linear optimisation that has computed a reasonable area which demonstrates that energy utilisation inside that area dependably encourages the network node to work for the maximal time. In [66] claimed that the investigation of the simulation results algorithm reduces the mean location error by 0.076–0.344 m on distinctive noise situations, as compared with the past LANDMARC algorithm; while the distance among tags is 1 m.

IV. CONCLUSION

The IoT is experiencing an unremitting rise within the ICT domain. IoT stands a huge chance of consistently blending reality and virtual worlds together through the monumental growth of surrounded devices—opening up new, exciting and challenging avenues for both research and business. This study mainly identifies different aspects of WSNs in IoT, and how IoT is going to be the primary focus of future technologies. The study also discusses different challenges which must be addressed when utilizing IoT. The simulation comparison results of security, privacy and STTS issues based on IoT smart environment monitoring systems will be indicated. Various research challenges have been recognised and cited, which are relied upon to trigger up significant research drifts. The most important application fields have been introduced and various utilised cases distinguished. Moreover, the study identifies the different features that IoT architecture can provide, particularly in terms of smart environment monitoring systems. This study would be valuable for analysts and professionals in this field of study, helping them to comprehend the vast capabilities of IoT, the significant issues to be handled, and methods for developing creative and urgent solutions that are integral and ready to turn IoT away from a mere theoretical abstraction into a reality within the real world.

V. ACKNOWLEDGMENT

The authors would like to acknowledge Universiti Sultan Zainal Abidin for the efforts, funds, and support for making this review paper successful.

REFERENCES

1. P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, “Wireless sensor networks A survey on recent developments and potential synergies,” J. Supercomput., 68(1), pp. 1–48, 2014.
2. D. B. Chen, N. L. Zhang, M. G. Zhang, Z. H. Wang, and Y. Zhang, “Study on remote monitoring system of crossing and spanning tangent tower,” IOP Conf. Ser. Mater. Sci. Eng., 199(1), 2017, pp. 1-6.
3. S. Sicari, C. Cappiello, F. D. Pellegrini, D. Miorandi, and A. C. Porisini, "A security-and quality-aware system architecture for Internet of Things," Information Systems Frontiers, 18(4), 2016, pp. 665-677.
4. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Ad Hoc Networks Internet of Things: Vision, applications and research challenges,” Ad Hoc Networks, 10(7), 2012, pp. 1497–1516.
5. S. Pirbhulal, H. Zhang, M. E. Alahi, H. Ghayvat, S. Mukhopadhyay, Y. T. Zhang, and W. Wu, “A novel secure IoT-based smart home automation system using a Wireless Sensor Network,” Sensors, 17(1), 2017, pp. 1–19.
6. V. J. Hodge, S. O’Keefe, M. Weeks, and A. Moulds, “Wireless sensor networks for condition monitoring in the railway industry: A survey,” IEEE Trans. Intell. Transp. Syst., 16(3), 2015, pp. 1088–1106.
7. H. H. A. B. Sidek, A. A. Jamal, M. Makhtar, and S. A. Fadzli, "Smart bicycle sharing system for non-commercial purposes using time-based one-time password algorithm," International Journal of Engineering and Technology (UAE), 7(3.28), 2018, pp. 275-277.
8. F. Viani, F. Robol, M. Bertolli, A. Polo, A. Massa, H. Ahmadi, and R. Boualleague, “A wireless monitoring system for phytosanitary treatment in smart farming applications,” IEEE International Symposium on Antennas and Propagation, 2016, pp. 2001–2002.
9. Z. Wadud, N. Javaid, M. A. Khan, N. Alrajeh, M. S. Alabed, and N. Guizani, “Lifetime maximization via hole alleviation in IoT enabling heterogeneous wireless sensor networks,” Sensors, 17(7), 2017, pp. 1–22.
10. L. Yu, Y. Lu, and X. Zhu, “Smart hospital based on Internet of Things," Journal of Networks, 7(10), 2012, pp. 1654-1661.
11. E. N. Mambou, S. M. Nlom, T. G. Swart, K. Ouahada, A. R. Ndjiongue, and H. C. Ferreira, “Monitoring of the medication distribution and the refrigeration temperature in a pharmacy based on Internet of Things (IoT) technology,” IEEE 18th Mediterranean Electrotechnical Conference, 2016, pp. 1–5.
12. Z. Butler, P. Corke, R. Peterson, and D. Rus, "Virtual fences for controlling cows," IEEE International Conference on Robotics and Automation, 2004, pp. 4429-4436.
13. Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, “A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems,” IEEE Commun. Surv. Tutorials, 19(1), 2016, pp. 550–586.
14. T. Arampatzis, J. Lygeros, S. Member, and S. Manesis, “A survey of applications of wireless sensors and wireless sensor networks,” IEEE International Symposium on Mediterranean Conference on Control and Automation Intelligent Control, 2005, pp. 719-724.
15. K. Øvsthus, and L. M. Kristensen, "An industrial perspective on wireless sensor networks-A survey of requirements, protocols, and challenges," IEEE Communications Surveys and Tutorials, 16(3), 2014, pp. 1391-1412.
16. Y. Zhu, J. Song, and F. Dong, “Applications of wireless sensor network in the agriculture environment monitoring,” Procedia Engineering, 16, 2011, pp. 608–614.
17. A. Milenković, C. Otto, and E. Jovanov, “Wireless sensor networks for personal health monitoring: Issues and an implementation,” Computer Communications, 29(13-14), 2006, pp. 2521–2533.
18. S. J. Isaac, G. P. Hancke, H. Madhoo, and A. Khatri, "A survey of wireless sensor network applications from a power utility's distribution perspective," IEEE Africon'11, 2011, pp. 1-5.
19. A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure localization algorithms for wireless sensor networks," IEEE Communications Magazine, 46(4), 2008, pp. 96-101.
20. H. Ning, and Z. Wang, "Future Internet of Things architecture: Like mankind neural system or social organization framework?," IEEE Communications Letters, 15(4), 2011, pp. 461-463.
21. H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, Vision and Challenges for Realising the Internet of Things. Brussels: European Commission, 2010.
22. C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “CA4IOT: Context awareness for Internet of Things,” IEEE International Conference on Green Computing and Communications, 2012, pp. 775-782.
23. O. Vermesan, P. Friess, and P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, and P. Doody, “Internet of Things strategic research roadmap,” Internet Things-Global Technol. Soc. Trends, 1, 2009, pp. 9–52.
24. I. Lee, and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” Bus. Horiz., 58(4), 2015, pp. 431–440.
25. E. Guillén, J. Sánchez, and C. O. Ramos, “A model to evaluate the performance of IoT applications,” International MultiConference of Engineers and Computer Scientists, 2017, pp. 15–18.
26. V. Hoyer and M. Fischer, "Market overview of enterprise mashup tools." International Conference on Service-Oriented Computing, 2008, pp. 708-721.
27. Y. Qin, Q. Z. Sheng, N. J. G. Falkner, S. Dustdar, H. Wang, and A. V. Vasilakos, “When things matter: A survey on data-centric Internet of Things,” J. Netw. Comput. Appl., 64, 2016, pp. 137–153.
28. J. Hradec, E. Pelikán, O. Mirovský, W. Pillmann, I. Holoubek, and T. Bandholtz, Proceedings of the European Conference Towards eEnvironment. Brno: Masaryk University, 2009.
29. E. Cero, J. B. Husić, and S. Baraković, “IoT’s tiny steps towards 5G: Telco’s perspective,” Symmetry, 9(10), 2017, pp. 1–38.

30. S. Kaur, and I. Singh, "A survey report on Internet of Things applications," International Journal of Computer Science Trends and Technology, 4(2), 2016, pp. 330–335.
31. H. Aly, M. Elmogy, and S. Barakt, "Big Data on Internet of Things: Applications, architecture, technologies, techniques, and future directions," International Journal of Computer Science Engineering, 4(6), 2015, pp. 300–313.
32. L. A. Amaral, E. D. Matos, R. T. Tiburski, F. Hessel, W. T. Lunardi, and S. Marczak, "Middleware technology for IoT systems: Challenges and perspectives toward 5G," in Internet of Things (IoT) in 5G Mobile Technologies, C. Mavromoustakis, G. Mastorakis and J. Batalla, Eds. Cham: Springer, 2016, pp. 333-367.
33. N. Xia, and C. S. Yang, "Recent Advances in Machine-to-Machine Communications," J. Comput. Commun., 4, 2016, pp. 107–111.
34. Q. Zhang, and F. H. Fitzek, "Mission critical IoT Communication in 5G," in Future Access Enablers of Ubiquitous and Intelligent Infrastructures, V. Atanasovski and A. Leon-Garcia, Eds. Cham: Springer, 2015, pp. 35-41.
35. Q. Song, L. Nuaymi, and X. Lagrange, "Survey of radio resource management issues and proposals for energy-efficient cellular networks that will cover billions of machines," Eurasip J. Wirel. Commun. Netw., 2016(1), 2016, pp. 1-20.
36. K. Zheng, F. Hu, W. Xiang, M. Dohler, and W. Wang, Radio resource allocation in LTE-advanced cellular networks with M2M communications. 2015, Available: https://arxiv.org/pdf/1510.06572.pdf.
37. O. Vermesan, and P. Friess, Internet of Things – From Research and Innovation to Market Deployment. Aalborg: River Publishers, 2014.
38. I. Lee, and K. Lee, "The Internet of Things (IoT): Application, investment, and challenges for enterprises," Bus. Horiz., 58(4), 2015, pp. 431–440.
39. A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a service and big data," International Conference on Advances in Cloud Computing, 2013, pp. 1-8.
40. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur Gener Comput Syst, 29(1), 2013, pp. 1–19.
41. V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: A survey," IEEE International Workshop on Security in RFID and Its Industrial Applications with IEEE 23rd International Conference on Advanced Information Networking and Applications, 2009, pp. 636–641.
42. M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 3(1), 2013, pp. 45-54.
43. J. Cabra, D. Castro, J. Colorado, D. Mendez, and L. Trujillo, "An IoT approach for wireless sensor networks applied to e-health environmental monitoring," IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2017, pp. 578–583.
44. Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. D. Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," IEEE Trans. Ind. Informatics, 10(2), 2014, pp. 1417–1425.
45. S. Fang, L. Xu, H. Pei, Y. Liu, Z. Liu, Y. Zhu, J. Yan, and H. Zhang, "An integrated approach to snowmelt flood forecasting in water resource management," IEEE Trans. Ind. Informatics, 10(1), 2014, pp. 548–558.
46. Z. Bi, L. Da Xu, and C. Wang, "Internet of Things for enterprise systems of modern manufacturing," IEEE Trans. Ind. Informatics, 10(2), 2014, pp. 1537–1546.
47. S. R. Prathibha, A. Hongal, and M. P. Jyothi, "IOT based monitoring system in smart agriculture," IEEE Int. Conf. Recent Adv. Electron. Commun. Technol., 2017, pp. 81–84.
48. W. Ejaz, and M. Ibnkahla, "Multiband spectrum sensing and resource allocation for IoT in cognitive 5G networks," IEEE Internet Things J., 5(1), 2018, pp. 150–163.
49. J. Henkel, S. Pagani, H. Amrouch, L. Bauer, and F. Samie, "Ultra-low power and dependability for IoT devices (Invited paper for IoT technologies)," IEEE Design, Automation and Test in Europe Conference and Exhibition, 2017, pp. 954–959.
50. Y. Nishiyama, M. Ishino, Y. Koizumi, T. Hasegawa, K. Sugiyama, and A. Tagami, "Proposal on routing-based mobility architecture for ICN-based cellular networks," IEEE Conference on Computer Communications Workshops, 2016, pp. 467-472.
51. I. Grønbæk, "Architecture for the Internet of Things (IoT): API and interconnect," IEEE 2nd International Conference on Sensor Technologies and Applications, 2008, pp. 802-807.
52. A. Mondal, and S. Bhattacharjee, "A reliable, multi-path, connection oriented and independent transport protocol for IoT networks," IEEE 9th International Conference on Communication Systems and Networks, 2017, pp. 590-591.
53. S. Sicari, A. Rizzardi, L. A. Grieco, and A. C. Porisini, "A secure ICN-IoT architecture," IEEE Int. Conf. Commun. Work., 2017, pp. 259–264.
54. S. Chatterjee, A survey of Internet of Things (IoT) over Information Centric Network (ICN). 2018, Available: https://www.researchgate.net/profile/Subhajit_Chatterje/publication/326987774_A_Survey_of_Internet_of_Things_IoT_over_Information_Centric_Network_ICN/links/5b70cc46a6fdcc87df73379c/A-Survey-of-Internet-of-Things-IoT-over-Information-Centric-Network-ICN.pdf.
55. A. R. Sadeghi, and C. Wachsmann, "Security and privacy challenges in industrial Internet of Things," 52nd ACM/EDAC/IEEE Design Automation Conference, 2015, pp. 1–6.
56. H. Mikko, and L. Nyman, "The Internet of (Vulnerable) Things: On Hypponen's law, security engineering, and IoT legislation," Technology Innovation Management Review, 7(4), 2017, pp. 5-11.
57. C. Mcphee, "Editorial: Insights," Technology Innovation Management Review, 8(5), 2018.
58. D. Shin, "Telematics and Informatics A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things," Telemat. Informatics, 31(4), 2014, pp. 519–531.
59. D. H. Shin, and Y. J. Park, "Understanding the Internet of Things ecosystem: multi-level analysis of users, society, and ecology," Digit. Policy, Regul. Gov., 19(1), 2017, pp. 1–26.
60. D. Childs et al., "HPE Security Research - Cyber Risk Report 2015," p. 76, 2015.
61. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," IEEE Symp. Secur. Priv., 1996, pp. 164–173.
62. A. Diaz, and P. Sanchez, "Simulation of attacks for security in wireless sensor network," Sensors, 16(11), 2016, pp. 1-27.

63. A. Mathur, T. Newe, and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT," Sensors, 16(1), 2016, pp. 1-25.
64. F. Österlind, A sensor network simulator for the Contiki OS. 2006, Available: http://soda.swedish-ict.se/2296/1/SICS-T--2006-05--SE.pdf.
65. S. Rani, R. Talwar, J. Malhotra, S. H. Ahmed, M. Sarkar, and H. Song, "A novel scheme for an energy efficient Internet of Things based on wireless sensor networks," Sensors, 15(11), 2015, pp. 28603–28626.
66. T. Zhang, Z. Chen, Y. Ouyang, J. Hao, and Z. Xiong, "An improved RFID-based locating algorithm by eliminating diversity of active tags for indoor environment," Comput. J., 52(8), 2008, pp. 902–909.