Internet of Things Based Secured Ground Water Level Monitoring System

[1] Mr. Akash Mishra, [2]Dr. Alok Mishra, [3]Dr. Pankaj Prajapati, [4]Dr. Rajeev Kumar Tripathi
[1]*M.Tech Scholarship, Ambalika Institute of management and technology, Lucknow*
[2]*Professor, Ambalika Institute of management and technology, Lucknow*
[3]*Associate professor, Ambalika Institute of management and technology, Lucknow*
[4]*Associate Professor, DAV Degree College, Lucknow*

***Abstract*— The main problem with some people is that they are lacking in people's consciousness Use of groundwater. Therefore, these are part of the process of designing an "application". Providing buyers with facts about groundwater abstraction, Use of groundwater by the purchaser. Also, while using most of the water, or Waste of water. This device sends water usage statistics for this location and automatically recorded with the amount of water by the local water department If used, the limit is exceeded, the locking device can also discharge the used water.**

Index Terms: **IoT, Arduno, Sensor, IoT Security**

1.INTRODUCTION

of the downpour water that penetrates below the floor`s floor, both usually or falsely, turns into groundwater. The relaxation of the little bit of the precipitation is used by plants, dissipates, or turns into floor water spillover that can both upload to groundwater tiers in unique territories or be accelerated with the aid of using groundwater outpourings depending upon the geography the floor water voyages through. The degree of precipitation that receives assimilated and turns into groundwater is based upon the dust type [1 2]. Highly permeable soils, for example, sandy soils, keep water lots faster than soil, for example, dust which has little pores. The immersed soil acts like a wipe and the vicinity in which groundwater is available, or soaked, within side the dust are known as a spring, which for the maximum component has a restriction characterized as its basin [34]. Groundwater bowls are framed usually over a duration strolling from pretty some time to over 1000 years in positive topographies. Groundwater is fundamental to the networks which are primarily based totally on or method the spring or the underground layer of water that fills splits within side the stone or sand that makes up the soil. This groundwater layer which makes up round 30 percentages of the worlds freshwater gracefully used for positive, motives such as water framework, nonpublic ingesting water, and metropolitan water supplies. Groundwater is a key little bit of the USA cap potential to flood its farmland. Water system talk to using approximately 53.three billion [5] gallons of groundwater always for agriculture watering. This usage may be regarded in a different way with regards to the 1900s whilst the United States clearly used 2.2 billion [6] gallons for water system. Furthermore the creatures and aquaculture ventures devour up commonly three.2 billion [7] gallons of groundwater always. Information as for groundwater use for ingesting water commonly talking is limited, anyways it`s far surveyed that 33% [89] of the all out human beings rely on groundwater because the crucial wellspring in their ingesting water. More than 13 million US nuclear households generally rely on nonpublic floor water wells. Groundwater purification It is used in about 33 percent [10] of the major water systems in the United States. Between open and private Wells About 44% of Americans rely on groundwater for water intake. Count near various jobs in groundwater, absorb water and grow. B. Collect, Mining and thermoelectric potential to present several models, 79.6 billion gallons new daily we use groundwater.

2. LITERATURE REVIEW

Knowing the groundwater stage is noteworthy for multiple reasons, which include understanding spring stages beneathneath static situations and siphoning

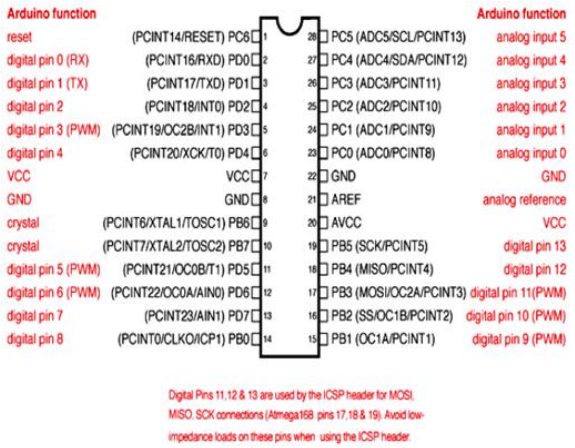
situations, selecting how the stages accomplice with close with the aid of using floor water sources, and perceiving how floor headway has stimulated the spring. Groundwater extraction from siphoning groundwater for floor use has the quality impact on the percentage of groundwater [11-12] set apart in a spring and the price at which it finishes off or energizes. The maximum critical final results of over the pinnacle groundwater siphoning are that the water desk may be lowered. It is crucial to display and realize the groundwater stages lawsuits uninteresting any wells that allows you to have noteworthy draw down of the spring since the water desk stages will deliver a clever thought of the impact of the brand new properly. For water to be pulled returned starting from the maximum punctual stage, must be directed from a properly that compasses below the water desk [13-14]. The records assembled with the aid of using checking groundwater may be used to select the percentage of groundwater that may effectively be pulled returned earlier than no extra water may be siphoned. Close with the aid of using water managers can guard wells from going dry and preclude the development of regularly disastrous nice groundwater into the spring. In the occasion that groundwater stages decline exorbitantly [15] far, with the aid of using then the properly proprietor can also additionally want to increase the properly, drill some other properly, or, at any price, try and reduce down the siphon which can emerge as being high-priced for the proprietor. Despite the value of extending the importance of the properly, getting into some other properly, or shifting the direct down because the importance to water constructs; the water need to now be lifted better to upward push to the pinnacle. Sometimes there can be a hazard that siphons are used to boost the water (in place of artesian wells), more essentialness is needed to force the siphon which realizes constantly exorbitant water. In the stop a substantial properly may want to emerge as being prohibitively high-priced to siphon water from. Certain areas lowering the water desk stage can significantly have an effect on the groundwater`s nice. In waterfront freshwater spring`s salt water interruption can appear whilst the diverse densities of each the saltwater and new water allow the ocean water to barge in into the brand new water aquifer [16-17]. Often beach the front groundwater springs bolster big populaces in which the hobby for groundwater withdrawals surpasses the brand new water revive price allowing salt water to strengthen into the spring sullying the water. Worldwide Positioning System (GPS) and close by situating calculations may be applied to acquire location and situating records of water. By which the place of the water frame with the waft price is proven in cellular simply. The sensor is used to discover the Moisture content material and Temperature of the sure location in the underground water and whilst the restriction exceeds the Notification is dispatched to the Customer and Government water board automatically.

3. PROPOSED SYSTEM

3.1 Water Level Sensor Water stream sensor comprises of a plastic valve from which water can pass. Water pivots alongside a Hall Effect sensor that sense and measures the water stream [18-19]. The fundamental working guideline behind the working of this sensor is the Hall Effect. As per this standard, in this sensor, a voltage distinction is instigated in the conductor because of the revolution of the rotor. This initiated voltage distinction is transverse to the electric flow.

Figure: 1.Water flow sensor

Figure: 2Arduino-UNO



GPS (Global Positioning System) that's used to discover the region of the underground sparkling water availability via way of means of storing the complete statistics via way of means of this task within side the Cloud Computing Technology. The Application affords the Guidance with the Data of water in that region visually to the human beings in "Google Map"and it assist electricity conserved and applied efficiently [20]. The restriction of the water is about in accordance to the water availability and exceptional of water to alarm over utilization facts to the human beings and Water Board via way of means of measuring the water float using "Arduino & Sensors". Peoples are usually For example deforestation, depleted wetlands, and concrete development motive water to overflow lots faster than it'd normally. This activates dwindled charging of the essential aquifer. The floor water collaboration referenced earlier than greater issues include the elevated price of water and land subsidence. The price of water increments because the profundity of the water desk increments due to costs associated with the energy required to raise the water further. Land subsidence, or soaking in, is introduced approximately via way of means of the loss of assist underground. Groundwater extraction can motive subsidence via way of means of leaving a void wherein the water was and drying the dust allowing it to shrivel and settle. As groundwater is steadily eliminated from the dust the opportunity builds that the floor will settle to occupy the unfilled areas left behind. This settling may be the wellspring of massive damage to the close by networks remembering breaks for establishments, dividers, streets or in all likelihood even sinkholes. It is essential to decide the Powerful groundwater looking is the quality manner to cope with secures the neighborhood system, make certain a reliable and realistic groundwater gracefully, and assure the sum to be had for sooner or later later [21]. Help line provision with Water Board Advice additionally to be had. The GPS (Global Positioning System) is applied to apprehend the region of the water frame with the subtleties is related to the Google Map secretly. This configuration makes it feasible for the Raspberry pi sensor dispatched the statistics to the Government whilst the water is over utilized or squandered [22].

4. DEFINING THE IoT THREAT LANDSCAPE AND SOLUTION REQUIREMENTS

IoT expands the hazard panorama and assault surface. Beyond sincerely the dangers of leveraging community endpoints without manage over safety measures, IoT offers 4 essential dangers safety experts need to understand of in growing a safety technique and defining answer necessities: Vulnerabilities—IoT gadgets are frequently now no longer designed or deployed with safety in thoughts. Some are even taken into consideration "headless," without the cap potential to run safety protocols or be up to date. Companies by no means predicted a printer or a thermostat being concerned in a botnet assault. But it has already happened. Also, even gadgets in which safety become taken into consideration can`t without difficulty be diagnosed or up to date within side the area to cope with new threats. How will you set up a method to identify, categorize, and manage new gadgets? Unsecure Communications—Devices leveraging public networks frequently speak without encryption and ship records on unprotected networks. Traffic is unmonitored, unmanaged, and unprotected. Public Wi-Fi and new approaches that leverage Bluetooth are of precise concern. Are you defining your IoT safety necessities with get admission to exposures in thoughts like public Wi-Fi? Data Leaks—IoT gadgets constitute an unsupervised and unmanaged entrance and go out factor to the community. As such, guidelines set to save you records leaks can also additionally fail to flag records passing via those gadgets. Devices need to be delivered into the larger community fold for guidelines to be enforced. How will your answer follow and enforce Answering these threat questions will provide a starting point for

security professionals to define the requirements of an IoT security solution. Transforming the IoT frontier into a hardened perimeter or at least gaining the visibility to see threats coming and be able to react to and prevent an attack is the baseline for any new solution.

5. CRITICAL ELEMENTS OF THE IoT SECURITY SOLUTION

To manage risk, security professionals must exert a degree of control over IoT infrastructure or, at the very least, its communication with the network. Three strategic areas must be addressed when developing solution requirements to minimize these threats: Learning, Segmentation, and Protection. LEARNING In the age of IoT, it may very well be that the network perimeter cannot be defined. For the secure enterprise, however, visibility is everything. This may be as simple as seeing a new employee's laptop power on and loading the appropriate security patches automatically. It might mean auto configuring access to a software program with a credential-based user policy. The critical piece is that the network must be aware of devices communicating on the network and be smart enough to know how to classify and learn how best to secure them. Without the capability to learn about devices, intelligent threat protection is impossible. When evaluating a solution, look for functionality in two key areas: Device Identification and Discovery—If you are like most organizations, a full view of every device on the network from a single dashboard is elusive. And the moment that snapshot is complete, it often changes. A solution must be able to automatically detect, profile, and classify what's on the network and develop a comprehensive inventory of devices. Once detected and profiled, security teams will be able to answer questions such as: What's the OS and how is it configured? Is the device managed? Is it trusted or rogue? Once discovered and visible, the proper policies can be applied. Predictive Action—The next challenge is to learn behaviors and predicatively react to an attack before it happens. For example, by classifying a device in terms of three categories—Managed Devices (the devices you control), Allowed Devices (the ones you accept but don't control), and Rogue Devices (suspicious devices not in policy compliance)—the fabric can learn the normal baseline activity for each category. This also helps in assigning a risk score to a device for segmentation and policy purposes. Once the normal behavior is known for these categories, the fabric can monitor for anomalies that will be more easily recognizable, whether it's a policy violation, unusual traffic for the time of day, or systems communicating that don't usually need to. Only with visibility at the macro level, across all categories of device, can an intelligent fabric learn to adapt and take action, becoming more predictive over time.

SEGMENTATION Segmenting the network and devices is about assigning policies and managing risk. When countermeasures fail in a more vulnerable or less critical part of the network, segmentation also protects more critical areas from being compromised. When defining solution requirements, security professionals must have the ability to manage policies, gain insight, and see trends based on risk profiles and type of infrastructure. Consider functionality in three areas when defining requirements for segmentation: Identifying Risk—The first order in segmentation is classification. Users, data, devices, locations, and a host of other criteria must be used to identify categories and assess risk. Systems that hold customer or financial data, for example, should be grouped with the network resources that directly access those systems. Managing Policies and Devices—As the network fabric expands, new devices must be not only discovered but configured based on existing device policies. A solution must provide the granularity to see all device activity and set policies appropriately. The fabric should know that when a new switch goes live, it will automatically inherit predetermined security policies. Networks grow too fast for this to be a manual process. A solution must have the flexibility to set policies by type of device or by users, traffic type, or perhaps even traffic by location or time of day. Policies should be the vehicle by which security professionals manage risk across the network. Exerting Control—Once an intruder gains access, an attacker could roam the network for weeks before acting. Segmenting the network, for example, isolating IoT devices and the other devices, servers, and ports they communicate with, allows the organization to separate resources on a risk basis. Choosing to treat parts of the network that interact

with IoT devices differently from a policy standpoint allows the organization to control risk. This type of solution can secure critical network zones and grant IoT devices privileges, based on their risk profile, without compromising other segments of the network.

PROTECTION The mission in IoT security is to first protect the device, then protect the network. Once an IoT device is secured and becomes part of the network, it must be protected in a coordinated fashion with all other network elements. Protection in the IoT realm becomes a matter of policy enforcement. When considering an IoT security solution, focus on one that can flexibly apply policy and enforce policy with automation across the following areas: Policy Flexibility and Enforcement—A flexible solution will have the ability to define and enforce policies on multiple levels across both type of device and access. To meet the challenges of IoT, rules must be enforced governing device behavior, what kind of traffic a device is allowed to generate, where it can be on the network, and even whether it can be on the network at all. BYOD, social media applications, and cloud-based applications are all examples where different policies must be established and enforced. Threat Intelligence—Once controls are established, a solution must be able to consistently enforce policies and translate compliance information across the network to all devices to create an intelligent fabric capable of learning and responding to threats. A solution where this intelligence is distributed throughout the security fabric ensures that the actions taken will be as close to the threat as possible. Even further, this threat intelligence should be capable of soliciting information from sources globally, including from other vendors, to identify threats before they happen and connect the dots with trending and threat information from inside the network. For a comprehensive solution, IoT devices must be subject to the same multilayered monitoring, inspection, and enforcement policies as the rest of the devices on a distributed network. Only then can all parts of the network communicate with each other to share policy information and threat intelligence and protect application data.

5. RESULTS

The consumer can view their water consumption through the application shown below and they can communicate to water board through it. It will useful for consumer and immediately they get consumption of water. The flow rate also can able to monitor with help of internet of things. The proposed method is simulated and hardware is implemented [23].

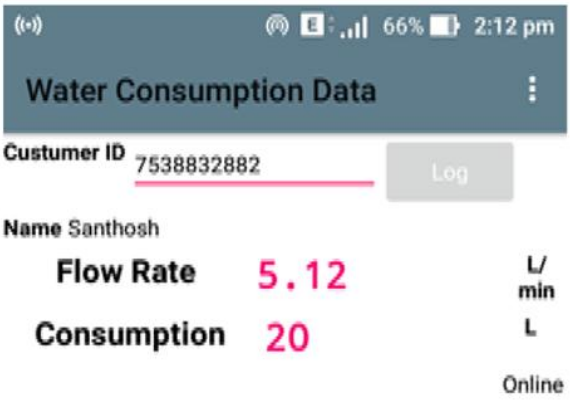


Figure: 5. Results of the Arduino based water monitoring system

6. CONCLUSION

In this paper, a model brilliant groundwater level observing framework utilizing Arduino is introduced. For this a few sensors are utilized. The gathered information from the all the sensors are utilized for investigation reason for better arrangement of water level just as stream rate checking can be executed. So this application will be the best challenger continuously checking and control framework and use to comprehend all the groundwater level observing related issues.

IoT will cause a sea change in the way businesses leverage data to make decisions, and in the way we manage our personal lives. This change will also require a rewriting of the network security playbook. When defining the requirements for an IoT security solution, firms must consider an approach anchored with an intelligent, network-wide security fabric that can learn and share information. This new approach must accept that when there is no clear delineation between the network and the outside world, everything that touches the network must be visible. We must assume that all devices at the edge and the core are vulnerable, regardless of how effective we view our perimeter defenses. We must understand that when threats can come from any direction or any

source, only an approach that allows us to see everything, segment based on risk, and teach the network to defend itself through intelligence and automation will help us to successfully navigate the waters of IoT security. With this IoT security solution requirements primer as a guide, IT security professionals can demand solutions that look at security holistically, recognizing that IoT devices, like all other elements of the network, must be visible, segmented, and protected.

REFERENCES

[1] Alessio B, Walter D, Valerio P, Antonio P, "Integration of Cloud computing and Internet of Things: A survey", Futur Gener Comput Syst 56: pp. 684–700, 2016.

[2] K. Xu, Y. Qu, K. Yang,"A tutorial on the Internet of Things: From a heterogeneous network integration perspective",IEEE Netw., Vol. 30, No. 2, pp. 102-108, 2016

[3] Prachet Verma, Akshay Kumar, Nihesh Rathod, Pratik Jain, Mallik Arjun, Renu Subramanian,"Towards an IoT based water management system for a campus", IEEE 2015

[4] Al-Fuqaha A et al,"Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Commun Surv Tutorials 17(4), pp. 2347–2376, 2015

[5] Thinagaran Perumal, Md Nasir Sulaiman, Leong.C.Y, "Internet Of Things (IoT) enabled water monitoring system", 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)..

[6] Prachet Varma, Akshay Kumar, Nihesh Rathod, Pratik Jain, Mallikarjun S, Renu Subramaniyam, Bhardhwaj Amrutur, M.S.Mohan Kumar, Rajesh Sundresan,"IoT based water management System for a Campus IEEE", IEEE First International Smart Cities Conference (ISC2), 2015.

[7] Perumal, T.; Sulaiman, M.N.; Mustapha, N.; Shahi, A.; Thinaharan, R., "Proactive architecture for Internet of Things (IoTs) management in smart homes," Consumer Electronics International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 10 | Oct 2018 www.irjet.net p-ISSN: 2395-0072 © 2018, IRJET | Impact Factor value: 7.211 | ISO

[8] V. Jayakumar, DC.Kumaresan, R.Karthikeyan "Wind Energy Conversion System and Solar PV Integration" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7, 1595-1600, May, 2019.

[9] V. Jayakumar, PL. Somasundaram "Implementation of single phase improved inverter for PV source", International journal of pure and applied mathematics JARIIE-ISSN(O)-2395-4396 Volume 4 No. 3 2018, 118 – 126

[10] S K Saranya & Dr R Karthikeyan "Security for Smart Distribution Grid by Using Wireless Communication", International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Volume 02 Special Issue 01 March 2014, pp: 01 – 09, ISSN: 2320-9801.

[11] Saima Maqbool, Nidhi Chandra,"Real Time Wireless Monitoring and Control of Water Systems using Zigbee 802.15.4", 5th International Conference on Computational Intelligence and Communication Networks, 2013.

[12] Asaad Ahmed Mohammed Ahmed Eltaieb, Zhang Jian Min,"Automatic Water Level Control System", International Journal of Science and Research (IJSR) 2013.

[13] A. T. Sankara Subramanian, P. Sabarish, M. D.Udayakumar and T. Vishnu kumar," Performance Analysis of Various Photovoltaic Configurations under Uniform Shading and Rapid Partial Shading Formations", Biosc.Biotech.Res. Comm. Special Issue Vol 13 No (3) 2020 Pp-185-192.

[14] P. Sabarish et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 623 012011.

[15] M D Udayakumar et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 623 012018.

[16] P. Sabarish, A. T. Sankara Subramanian, S. Murugesan and V. Sureshkumar, "A New Methodology of Arterial Blood Clot Removal Using Bio Molecular Devices for ATPase Nuclear Motors." Biosc.Biotech.Res.Comm. Special Issue Vol 13 No (3) 2020 Pp-197-201.

[17] Karthick, R and Sundararajan, M. (2017), "Design and Implementation of Low Power Testing Using Advanced Razor Based

Processor," International Journal of Applied Engineering Research, 12.

[18] Karthick, R and Sundararajan, M. (2018), "A novel 3-D-IC test architecture-a review," International Journal of Engineering and Technology (UAE).

[19] A Nazar Ali, D Sivamani, R Jaiganesh M Pradeep (2019), Solar powered air conditioner using BLDC motor, IOP Conference Series: Materials Science and Engineering, vol. 23.

[20] V Venkatesh, A Nazar Ali,, R Jaiganesh. V Indiragandhi (2019), Extraction and conversion of exhaust heat from automobile engine in to electrical energy Energy, IOP Conference Series: Materials Science and Engineering, vol. 23.