International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-7, May 2020

AIoT with PUF: A Concrete Security

Harsha Patil, Deepashree Mehendale, Malati Tribhuwan, Vidya Bankar, Satyawan Kunjir, Reshma Masurekar.

Abstract: ***Artificial Intelligence in contrast to Natural Intelligence also known as Machine Intelligence is intelligence revealed by machine. It is the science and engineering of making machines intelligent. Therefore, it is a technique that makes a machine work like humans. The IOT Internet of Things is a network of internet-connected objects which can connect and exchange data. The combination of AI and IoT called AIoT is the combination of Artificial Intelligence and Internet of Things to achieve more efficient IoT operations. When Artificial Intelligence is added to IoT it means that the devices can analyze data and make decisions and act accordingly without the intervention of humans. The combination of AI and IOT has several advantages like saving money, building deeper customer relationships, increased operational efficiency and productivity and enhanced security and safety. This research paper focuses on what is AIoT, its applications and challenges and further, it also focuses on AIoT security concern and how can we solve the security problem with the use of PUF which is hardware security which is a simple and fast solution for security purpose. PUF is also more compatible with AIoT gadgets. Attacks on IoT devices are on the upsurge. Physical Unclonable functions (PUFs) are recognized as a robust and mild-weight way for AIoT.***

Keywords: Artificial Intelligence, Internet of Things, Intelligent Systems, PUF, AIoT.

I. INTRODUCTION

The term Artificial Intelligence was coined long back in the year 1956. It is the science and engineering of making machines intelligent. Artificial Intelligence has many advantages as it is one of the emerging technologies for a recent generation. It solves the problem of reducing human error, taking more risks that cannot be taken by humans, 24*7 availability, digital assistance, helping in repetitive jobs, etc. Internet of things commonly abbreviated as IoT is a network of connected objects which can collect and exchange data. IoT has various advantages like easily accessing information, better communication over a network, more cost-effective, privacy and security, increased efficiency of service, etc. As we see there are many pros of using IoT similarly there are also cons of the same as whenever we send data over network leakage of data is a major concern, as IoT structure is very complex a simple loophole can also put the entire system down affecting everyone.

The combination of AI and IoT is known as AIoT has a greater advantage. AI and IoT have their advantages when combined will give more benefits. It makes artificial intelligence and the Internet of things work together.AI can be used to transform IoT data into useful information which will help for a more improved decision-making process. AI adds value to IoT through machine learning capabilities and IoT adds value to AI through connectivity, signaling and data exchange. By some estimates, there will be more than 80 billion connected things producing more than 180 zettabytes of data annually by 2025. Bolder predictions have their sights set on IoT devices creating 847 zettabytes of data by 2021. Either way, it's a large number -- and one that is only going to grow. Its objective is to increase operational efficiency, improve human- machine interactions and upgrade data management and analytics.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Mrs. Harsha Patil*, Computer Science Department, Dr. D. Y. Patil ACS College, Pimpri, Pune, India. Email: hrpatel888@gmail.com
Mrs. Deepashree Mehendale, Computer Science Department, Dr. D. Y.PatilACSCollege,Pimpri,Pune,India.Email:deepashree.deshpande2@gmail.com
Mrs. Malati Tribhuwan, Computer Science Department, Dr. D. Y. Patil ACS College, Pimpri, Pune, India. Email: tmalativ@gmail.com
Mrs. Vidya Bankar, Computer Science Department, Dr. D. Y. Patil ACS College, Pimpri, Pune, India. Email: vidyabankar81@gmail.com
Mr. Satyawan Kunjir, Computer Science Department, Dr. D. Y. Patil ACS College, Pimpri, Pune, India. Email: ksatyavan1981@gmail.com
Mrs. Reshma Masurekar, Computer Science Department, Dr. D. Y. Patil ACS College, Pimpri, Pune, India. Email: rush1681@gmail.com

II. ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence is that the technological know-how of instilling intelligence in machines so that they may be capable of doing duties that traditionally required human thoughts. AI primarily based structures are evolving swiftly in terms of utility, variation, processing speed and abilities. Machines are more and more turning into able to take over many less-ordinary responsibilities. While human intelligence is 'taking' an ideal selection on the acceptable time, AI is clearly about 'choosing' a right selection on the desirable time. To area it seems that the creativity in a decision that humans can take is lacking in AI. It's going to be argued that human ingenuity will usually change the role of efficient work; however, AI-based systems have quite elegantly reduced the repetition of human efforts and will give ends in the comparatively low time. Most of the ongoing works in AI are often termed as 'slim AI'. This suggests that only sure tasks are superior through technology. But we're aiming for something far more than that. Consequently, many fields have conjugated to pressure the AI development. Intelligence comes from all the information generated in every of those domain names. Evaluation of these facts is critical to bring out the concepts at the back of it. The human mind can do it effortlessly, but it takes a prolonged time. This is regularly due to the fact, the info in global has a few unwelcome homes.

There are other homes too like volatility, virility, and so forth. AI is often taken into consideration a way to apply the information efficiently so that it's understandable to the human beings that provide it, modifiable (in case of errors), holds usefulness within the present situation and is meaningful.

III. INTERNET OF THINGS (IOT)

IoT is everything which is connected to the web, but it's increasingly getting used to define objects that "speak" to every other. By combining connected devices with automated systems, it's possible to "gather information, analyze it and make an action" to assist someone with a specific task or learn from a process, this ranges from smart mirrors to beacons in shops and beyond.

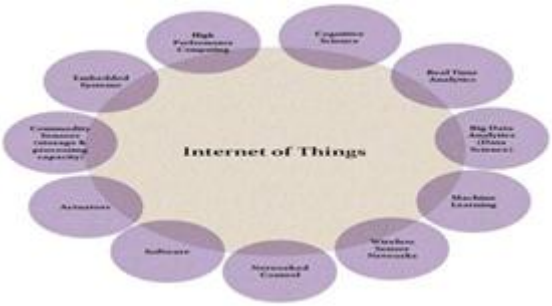

Fig. 1: Various fields merging in IoT

What we had on the grounds that 1991 become "internet of computer systems (IoC)" and it gradually grew in length as an increasing number of people began using it. IoT allows devices on closed private internet connections to speak with others and "the Internet of Things brings those networks together. It gives the chance for devices to speak not only within close silos but across different networking types and creates a way more connected world."

The Internet of Things, or IoT, refers to the billions of physical devices round the world that are now connected to the web, all collecting and sharing data. because of the arrival of super-cheap computer chips and therefore the ubiquity of wireless networks, it's possible to show anything, from something as small as a pill to something as big as an aero plane, into a neighborhood of the IoT. Connecting of these heterogeneous objects and adding sensors to them adds a level of digital intelligence to devices that might be otherwise dumb, enabling them to speak real-time data without involving a person's being. The Internet of Things is making the material of the planet around us smarter and more responsive, merging the digital and physical universes.

Internet of factors is genuinely a related machine of bodily matters (like home equipment, crop fields, plants, animals, and many others.) and people. Human beings are related to those gadgets using a few smart items connected to each which might be capable of sending, receiving and reading records.

A. Internet of Everything (IoE)

The Internet of Everything (IoE) may be a concept that aims to seem at the larger picture during which the web of Things fits. It is basically a philosophy during which our technology future is comprised of various sorts of appliances, devices, and things connected to the worldwide internet. Simply ,IoE is that the intelligent and cognitive connection which can be transforming our world in such how that there will be billions of connected devices having sensors to detect, measure and access their status all of which can be connected over public or private network built over standard protocols like TCP/IP. The Internet of Everything (IoE) could also be an idea that aims to look at the larger picture during which the online of Things fits. It is basically a philosophy during which our technology future is comprised of varied kinds of appliances, devices, and things connected to the worldwide internet. As of now the online connection is simply restricted to Phone's/Tablet's, PC's and a few of other devices but the thought behind IoE is that within the longer term , Machines become more intelligent and cognitive by having more access to data and expanded network opportunities.

In simpler terms IoE is that the intelligent connection of individual , process, data and things which can be transforming our world in such how that there will be billions of connected devices having sensors to detect, measure and access their status all of which may be connected over public or private network built over standard protocols like TCP/IP. IoE is that the intelligent connection of individual, process, data and things.

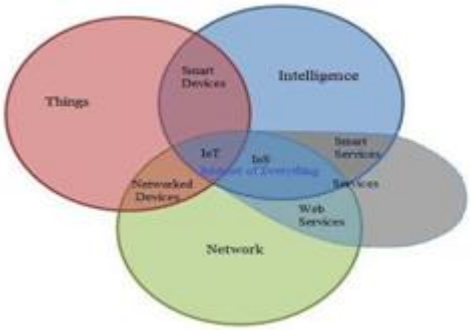

Fig. 2: Concept of Internet of Things (IoT), Internet of Services (IoS) and Internet of Everything (IoE)

B. Internet of Services (IoS)

The basic idea of Internet of Services is to systematically use the web for new as useful creation within the services sector. There are different angles from which one may check out this approach. From an IT perspective, service-oriented architectures, software-as-a-service, also as business process outsourcing are related trends. During this context, the concept of service is pertaining to a technical understanding of software functions provided as Web services. But services in a broader sense are quite technical capabilities which will be invoked by computer program interfaces. When pertaining to the importance of the services Therefore, it's important to clarify what we mean by the term service Here is our proposal for a definition: A service may be a commercial transaction where one party grants temporary access to the resources of another party so as to perform a prescribed function and a related benefit. Resources could also be human workforce and skills, technical systems, information, consumables, land etc.

For our part, the Internet of things (IoT) and AI (AI) are effective technologies. After combine AI and IoT, you will get AIoT—the AI of Things. You'll consider the internet of things gadgets because the digital machine apprehensive while AI is that the brain of a gadget.

IV. WHAT IS AIOT?

Artificial Intelligence of things (AIoT) is the aggregate of artificial Intelligence (AI) technologies and net of factors (IoT) infrastructure which more efficiently attains IoT operations, enhance the interplay between human and machine and beautify information management and statistics analytics which makes IoT smart. AIoT is mutually useful for both forms of era equally as AI provides a fee to IoT through machine gaining knowledge of competencies that analyzed and converts unstructured facts into useful records and IoT provides price to AI via connectivity, signaling and change of statistics.

In most of the industries that are the use of IoT, there might be a big quantity of human orientated and machine-generated unstructured facts. AIoT presents a guide for facts analytics solutions that could create price out of such unstructured records. There are many extraordinary applications across a couple of industries, offices, and homes that require artificial intelligence and internet of factors in combination, some of them are as follows:

A. Applications of AIoT

1) Smart Retail:

In smart retail gadgets, a digital camera is established inside save to understand the face of the customer through which it can accumulate required facts about consumers like the gender, age, products desired and visitors glide at the distinctive time and so forth. Then gadgets will efficiently analyze these facts with a purpose to help to predict the conduct of the clients exactly and in the end to enhance the boom of retail business by way of changing the strategies or offers to gain maximum earnings if required. Clever buying carts of patron have shown panels on it which offers them stay updates approximately classified ads or offers approximately products as they pass via a store. Similarly, it can find the issues faced with the aid of the customers to overcome them. A retail device with AIoT era can also apprehend robbery in save and block such clients from entering the shop inside the future.

2) Traffic monitoring using CCTV cameras and Drone:

Underneath smart city the use of AIoT way of tracking traffic has been modified, CCTV cameras mounted on-site visitors lighting fixtures data statistics about the vehicles like its pace, wide variety, model, type and if a person breaks a visitors rule the awareness with great receipt is sent to their residence. Here IoT is doing the job of recording data and AI algorithms are analyzing it to discover records approximately car proprietors like deal with, history, and the quantity that has to be charged as per the guideline that has been broken with the aid of the character.

In some countries clever towns, this traffic monitoring has gone even a stage better with the aid of doing it via the drone; the usage of this records device will adjust or exchange the timing of site visitors indicators without human involvement, to lessen congestion. Drones display a huge location as examine to CCTV cameras; they're no longer fixed and may flow to capture more information. The drones can also discover the injuries occurring in an area and with the assist of AIoT visitor's department can alternate their rules to lessen the accidents via taking vital measures. Car parking difficulty may be solved utilizing detecting unlawful parking through such a drone system.

3) Smart Office:

Office using AIoT, a community of smart environmental sensors can be established, for you to come across indoor brightness, temperature and the number of humans present in a workplace in actual time. Consistent with which brightness of indoor lighting, the air-conditioning temperature may be adjusted. If the device recognizes no-one is in office and still, lights are on, it's going to mechanically turn off or reduce the brightness of the light. This can store plenty of power and price to an exquisite extent and will also create an extra convenient and surroundings friendly smart office.

4) Management of fleet:

AIoT generation can also be used for the manager of a fleet; it may monitor the cars of a fleet, can lessen the rate of the fuel for them and also can music the automobile's renovation. Here in a vehicle GPS device is set up to tune the automobile and AI assist to come upon unstable conduct of driving force.

5) Management of Autonomous vehicles:

One extra application of AIoT is to manage self-reliant vehicles like the Tesla's autopilot systems, wherein they use the IoT gadgets radar era, GPS, and a few cameras to accumulate the information approximately the situations of using. AI generation is used to make similarly crucial decisions to help the autopilot system.

6) Autonomous Robots:

The autonomous robots have sensors set up in them to help them to gather essential information for their functioning and AI enables the robots to make decisions of their work as self-sustaining automobiles. These are surprisingly complicated machines that are designed to assist human beings in their office or industry or inns to fulfill tough obligations.

7) Automated vacuum cleaner:

Computerized or clever vacuum cleaner makes use of AIoT, set of sensors are used to discover boundaries, dirty spots at the floor or even steep drops consisting of stairs. It remembers the format of the house and then uses the most efficient and cost-effective movement sample for cleansing the house.

8) Smart Security System in office:

One more application of AIoT is to provide get right of entry to manage in sensitive regions of office via either fingerprint identity or face recognition of a person in which films and pix were taken in real-time and after right evaluation decision, approximately access is taken. AIoT makes it feasible for cameras to now not only file what a person does however also recognize who is that man or woman straight away.

In face recognition technology, the camera detects the features of a person's face and compares it with a database for matching purposes. The usage of such a system, for each day attendance or obligatory meeting attendance personnel, can test their faces as they walk with the aid of and their presence gets recorded robotically. It improves the accuracy of identification and gets rid of timesheet fraud which includes others punching or proxy attendance.

B. Introducing AIoT Trends

The artificial intelligence of things (AIoT) are often a replacement trend that mixes AI (AI) with the Internet of things (IoT) to form networks of virtual gadgets that communicate and procedure records. At an equivalent time as IoT creates full-size connections, AI makes these devices awaken. Right here's one example: an IP camera system is usually used for condo safety. But, without AI, humans got to display video from the device in actual time that permits you to reply to emergencies. With AI, IP cameras can recognize risks routinely and ship indicators. Truly, AIoT promises to grow hastily and affords rise to new high-cost merchandise within the identical manner that internet led to the introduction of various big corporations. people who input the meeting of AIoT gadgets are getting to be poised to faucet an enormous new marketplace. IoT devises today quantity within the billions. These small, linked gadgets contain digital gadgets and residential equipment networked collectively and communicating over internet protocols (IPs). But including AI to IoT has created new safety challenges.

C. The Challenges of AIoT

One of the key challenges for AIoT is that the security of AI belongings. AI capabilities frequently got to detect, examine and reply in actual time. As a result, an important protection challenge is that the undeniable fact that inner databases and interfaces for AI isn't suitable for encryption because such an operation might demand an excessive amount of time and sources. But huge facts and interface designs are all proprietary records that has got to be securely covered. the knowledge wanted by way of AI structures is usually so large that it always be saved in an external non-risky memory (NVM), thereby exposing it to hacking dangers which could be increasing global. within the meantime, additionally to the "inner" safety troubles with AIoT structures, the external challenges of AIoT safety have also elevated. Nearly two million cyber assaults in 2018 led to additional than $45 billion in losses global as governments struggled with ransom ware and other malicious incidents.

The net Society's online consider Alliance (OTA), which identifies and promotes safety and privations nice practices that construct purchaser confidence within the internet, stated in its Cyber Incident & Breach traits report that the financial impact of ransom ware rose by way of 60%, losses from commercial enterprise electronic message compromise (BEC) doubled, and crypto jacking incidents pretty tripled in 2018.It's clean that whilst protection issues remain unresolved, the deployment of AIoT gadgets will increase assault vectors for intrusions. Therefore, we are announcing that for AIoT gadgets, PUF-based hardware safety is the right solution.

D. Need of Security in AIoT

In this new generation, AIoT packages are getting greater famous, at the same time as using those applications agencies, people need to now not handiest don't forget how to procedure and analyze generated information but need to additionally deal with protection of facts because cyber criminals discover new hacking techniques to seize such sensitive information. As this information will become individual's maximum valuable useful resource, it also will become a sufferer for attackers round the arena. Imparting safeguards must be the priority even as the usage of packages which can be based totally on AIoT. Safety can be ensured by using proscribing get entry to to all associated assets like endpoints, offerings and statistics and to put into effect access manage, robust mutual authentication preferred cryptography techniques need to be applied. Ongreater technique to handle these assaults is to display and detect infected devices in real-time, and do not use such compromised devices. Due to the truth if a unmarried device is compromised, the complete community of that device receives right now exposed. We can without issue come upon behavioral anomalies of such device the use of AI and system learning algorithms.

Cellular gadgets, charge gambling playing cards and fee statistics all are being made available now to systems like Google and automated devices like Amazon's Alexa therefore generation needs to recognition on protection to defend the people and their facts in any other case attackers attempt to advantage get admission to and could try to manage such financial records. With AIoT generation in the healthcare agency, the dangers are focused on a person stage. Many devices are embedded-type devices that may be in or on the human frame and records stored with the aid of them is at risk of being accessed by way of the usage of attackers. Protection to such statistics can prevent unauthorized get proper of entry to, which sooner or later ought to result in a lifestyles or loss of life situation. Further clever domestic devices used expect someone's wishes thru monitoring the man or woman's interplay with the tool and recording it. This recorded information is similarly communicated to a server, however if communiqué hyperlink used is not secure then it will become an easy access factor for attackers to get into your private home. Statistics saved inside server ought to also be encrypted to keep away from further risk.

Now an afternoon thinking about the reality that more and more devices are linked to net and attacks are continuing to evolve more statistics may be compromised. We can use hardware in devices to comprise protection skills to strengthen the safety and integrity of the product or application. Unless hardware-based protection, solutions are applied in IoT and AI devices, clients go away themselves uncovered to cyber-attacks. More especially we will use computer chips that combine safety on the transistor degree, embedded in the processor, to offer encryption and anonymity.

Implementing the critical functionality on the gadget on Chip (SoC) diploma is a key detail of secure devices. On the facet of making sure important chip protection all through manufacturing if we embed a separate safety IP center into SoC then systems will continue to be comfortable during their lifecycles to shield blessings of IoT and AI.

V. PHYSICALLY UNCLONABLE FUNCTIONS (PUF)

Like human, each chip has its own fingerprint, that's created at some stage in manufacturing. This intrinsic feature is extractable by way of adding specific circuit structure, a so-known as PUF circuit, to the chip (see figure-3). PUF circuits acquire a chain of bits (alleged challenges) because the center and generate a sequence of bits (so-called responses) as the output. No two chips generate equal responses for a specific venture. The mixture of an assignment and its corresponding reaction is called a task response Pair (TRP).

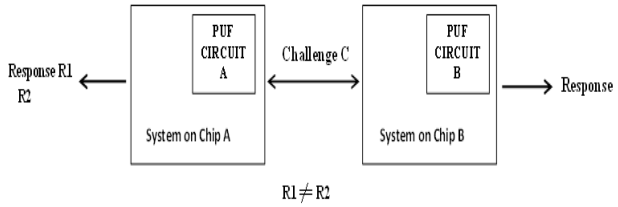

Fig.3: Two Similar PUFs Circuits on two different Chips Generate different response

PUFs usually are used for authentication and cozy verbal exchange. Due to the fact PUF- primarily based authentication does no longer require classical cryptographic belongings; it fits nicely into the aid demands of IoT gadgets. PUF authentication protocols have stages: the enrollment and the authentication phase. The primary proposed PUF-primarily based authentication protocol works as follows: all through the enrollment section (see figure-4a), the chip which contains the PUF circuit is immediately connected to the server. The server sends challenges, and the PUF circuit sends returned the responses. The server retains and stores all CRPs in a table. Then, the chip might be set up into the IoT tool. All through the authentication segment (see figure-4b), if the tool wishes to be authenticated by the server, the server sends an arbitrary PUF challenge to the device. Upon measurement of PUF, the device further sends back the generated response to the bits. If the measured reaction suits the stored reaction within the server database, then the tool is authenticated. Most of the traditional applications used by PUF are meant to extract key from the PUF response which results into encrypted communiqué.

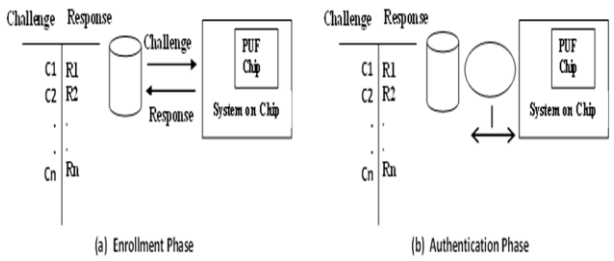

Fig.4: PUF Authentication Protocol

A. PUF Solves AIoT Security Concerns:

One of the challenges for adding security in an AIoT device is the way to do so without adding silicon land or cost, given the resource constraints in terms of keeping minimum power consumption and optimizing the processing resources on the device.

With an efficient implementation of PUF, it's possible to beat the bounds of conventional key storage: the PUF circuitry doesn't have A battery or other permanent power source. Attempts to physically probe the key will drastically change the characteristics of that PUF circuit and thus produce a special number. The PUF key can only be generated when it's needed for a cryptographic operation and may be instantly erased later.

PUF is a hardware security based totally on the physical unclonable variations taking place inside the silicon manufacturing system. The underlying advantage of the use of a PUF in cryptography is its "specialty" and "unpredictability". The random number extracted through PUF is so particular and unclonable that it can be used as a silicon "fingerprint" for an extensive variety of protection functions, which include encryption, identification, authentication and security key generation.

An attack on AIoT includes "facts and firmware attacks", "transmission attacks" and "facts integrity hit". The PUF technology provides advantages in terms of strong security of a tamper-proof SRAM. Although PUF technology alone isn't enough to make sure key security, it certainly minimizes the vulnerability of embedded devices. We cited that complex encryption and decryption are impractical for the safety of AIoT property. PUF has emerged as an exceptionally simple and rapid solution for safety.

VI. CONCLUSION

In this paper, we investigated PUF-based total authentication solutions in AIoT. Our focus becomes on AIoT gadgets that have energy and computational resource worries. We analyzed viable threats and how present-day PUF architectures, cope with them. We're locating that HW-based totally safety ICs is a longtime approach to guard your treasured application property from theft, snooping, counterfeiting, and lots of others. PUF era protects the security chip itself towards invasive kinds of attack threats. The random electrical residences of IC gadgets based on PUF technology, generates a singular and repeatable root cryptographic key for each IC. As a result, no PUF coding is that the equal. Moreover, the technology of a key takes place whilst needed, and therefore the chip never shops this valuable key. This removes any danger of destiny cyber-assaults. Reliability of your silicon may be a large order. Its miles essential that the PUF feature be dependable over voltage, temperature, time, procedure, and age. So, PUF is the key to deal with AIoT security concerns. PUF can reliably generate unique and unpredictable secret for highly secure and inexpensive hardware security solution in IC's. To use PUF-based hardware security solutions to protect AIoT's trust-worthy sustainable operation through life cycle has become the most urgent and important mission in AIoT era.

REFERENCES

1. Das, A.K.; Zeadally, S.; He, D. Taxonomy and analysis of security protocols for Internet of Things. Future Gener. Comput. Syst. 2018, 89, 110–125.
2. Pappu, S.R. Physical One-Way Functions. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2001.
3. Chatterjee, U.; Chakraborty, R.S.; Mukhopadhyay, D. A PUF-Based Secure Communication Protocol for IoT. ACM Trans. Embed. Comput. Syst. 2017, 16, 67.
4. Zheng, Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption). In Annual International Cryptology Conference; Springer: Berlin/Heidelberg, Germany, 1997; pp. 165–179.
5. Tashi, J.J. Comparative analysis of smart card authentication schemes. IOSR J. Comput. Eng. 2014, 16, 91–97.
6. Braeken, A. Efficient anonymous smart card based authentication scheme for multi-server architecture. Int. J. Smart Home 2015, 9, 177–184.
7. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In Workshop on the Theory and Application of Cryptographic Techniques; Springer: Berlin/Heidelberg, Germany, 1984; Volume 196, pp. 47–53.
8. Al-Riyami, S.S.; Paterson, K.G. Certificateless Public Key Cryptography. In International Conference on the Theory and Application of Cryptology and Information Security; Springer: Berlin/Heidelberg, Germany, 2003; pp. 452–473.
9. Gentry, C. Certificate-Based Encryption and the Certificate Revocation Problem. In International Conference on the Theory and Applications of Cryptographic Techniques; Springer: Berlin/Heidelberg, Germany, 2003; pp. 272–293.
10. https://www.edn.com/puf-up-your-iot-security/
11. https://www.forbes.com/sites/bernardmarr/2019/12/20/what-is-the-artificial-intelliigence-of-things-when-ai-mets-iot/
12. https://www.designreuse.com/articles/46928/puf-a-crucial-technology-for-ai-and- iot.html
13. https://www.edn.com/puf-up-your-iot-security/
14. https://www.forbes.com/sites/bernardmarr/2019/12/20/what-is-the-artificial-intelligence-of-things-when-ai-meets-iot/
15. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

AUTHORS PROFILE

Mrs. Harsha Patil. MSc (CS), NET
Assistant Professor Dr. D. Y. Patil ACS College Pimpri, Pune-18.

Mrs. Deepashree Mehendale. MCS, NET
Assistant Professor Dr. D. Y. Patil ACS College Pimpri, Pune-18

Mrs. Malati Tribhuwan. MSc (CS)
Assistant Professor Dr. D. Y. Patil ACS College Pimpri, Pune-18

Mrs. Vidya Bankar. MCS, NET
Assistant Professor Dr. D. Y. Patil ACS College Pimpri, Pune-18

Mr. Satyawan Kunjir. MCS, NET
Assistant Professor Dr. D. Y.Patil ACS College Pimpri, Pune-18

Mrs. Reshma Masurekar. MCS
Assistant Professor Dr. D. Y.Patil ACS College Pimpri, Pune-18