Study on Security and Privacy Approaches on Pervasive Computing Environment

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

[1] PhD Student, Kalinga University, Raipur

[2] PhD Guide, Kalinga University, Raipur

Abstract – It is not necessarily the case that all components in this conveyed situation should be portable—just that no specific arrangement of gadgets/PCs is accessible to frame the steady center of an appropriated framework consistently. For example, in environments like shopping centers, gathering scenes, or shrewd workplaces, a few gadgets (e.g., work areas/workstations, IP telephones, retail location terminals, projectors, espresso machines) are static while different gadgets (PDAs, handhelds, and so forth) are versatile. In the limit case, Pervasive Computing environments incorporate MANETs (Mobile Ad hoc Networks), where all hubs are versatile and progressively change their areas. Instances of such environments can be found in the cell phones utilized by crisis reaction administrations, by officers in combat zones, by individuals strolling on roads, and so forth.

Keywords – Computing, Environment, Portable, Mobile Ad hoc Networks

- x -

INTRODUCTION

The meshing of the significant advances into the texture of regular day to day existence was a fantasy of Weiser so they break down and get indistinct. In 1991, the exploration paper of Mark Weiser plainly portrayed his vision of universal computing, where shrewd spaces break up in the pervasive environment, subsequently clearing path for more work and developmental strides in this area of Pervasive Computing Environment (PCE). In Pervasive computing, instead of having PCs as particular items, it is unfurling the idea of incorporating calculation into the environment.

Advertisers of this idea accept that implanting calculation procedures into the environment empowers public to move around and collaborate with PCs all the more unhesitatingly. The development in the present data innovation is to such an extent that we are moving towards an environment of installed gadgets and availability which imperceptibly turns into a portion of human cooperation consistently so clients begin utilizing the innovation effortlessly, similar to some other day by day movement. Despite the fact that the pervasive computing can make day by day exercises quicker and cost productive, these frameworks present test for protection and security issues and make questions encompassing client accord. For instance, in a house expanded situation of Pervasive Computing Environment, shrewd lighting and cooling frameworks could contact through sensors to control the house inhabitant's practices and screen their solace levels. There exists many confirming conventions and in some cases existing confirmation conventions can't give total security to these pervasive computing gadgets and need more powerful and solid methods that can make the basic brilliant gadgets and items secure.

Pervasive computing innovation means to work on regular daily existence by giving portable clients to convey individual and business administrations across versatile and installed gadgets. Such developments guarantee to support usefulness through consistent cooperations, permitting admittance to applications and benefits and establishing shrewd homes and environments at whenever and anyplace. Because of late advancements in versatile minimal expense lightweight gadgets and the rise of short-reach and low-power remote correspondence organizations, pervasive computing has developed in the course of recent years for the combination of innovation and connection with the basic actual environment of regular day to day existence. From a wide perspective, pervasive computing covers four fundamental regions: versatile computing, remote organizations, inserted computing and setting mindful sensor organization. There are different gadgets in the omnipresent computing environment that incorporate PDAs, PDAs, advanced mobile phones, workstations, sensors, and so forth which

make Weiser's vision a reality all over the place. There are various sorts of organizations in pervasive computing environment. There are networks that are upheld by fixed passages or focal workers, yet are not piece of a shrewd space. Computing is not, at this point a discrete movement bound to a work area; network computing and versatile computing are quick turning into a piece of regular day to day existence as is the Internet. Maybe than being a framework for PCs and their clients alone, it is presently a foundation for everybody. Gadgets like PDAs (Personal Digital Assistants), cell phones, workplaces PCs and surprisingly home theater setups may get to data and work together in one incorporated framework and the test is to consolidate these advancements into a consistent entire on the Internet.

MOTIVATION

Many a times, problems are faced due to poorly defined security parameters in any conventional office especially in the domain of user authentication and device utilization. Conventional methods for authentication focusing on security issues are context-insensitive and are not able to adapt to the rapidly changing need of context parameters. Therefore, flexible trust-based authentication needs to be addressed to convert a conventional office into smart office.

Smart Office

An office space loaded up with IoT gadgets is frequently alluded to as a brilliant office. This addresses a computerized biological system that depends on an assortment of associated gadgets that track, control and oversees various activities and working conditions. Savvy office innovation is intended to improve the general environment by expanding the effectiveness, security and solace. A savvy office is a work environment where innovation makes it feasible for individuals to work better, quicker and more astute. Guides, sensors and portable applications assist workers with performing manual errands better and quicker.

Designing also assist individuals with conveying a brilliant work environment. Sensors tell if an individual is in the structure, unequivocally where they are out of nowhere.

1) **IoT Sensors:** Using the Internet of Things (IoT) sensors is the core of smart office technologies. Such sensors are systems that use indoor motion detection to detect movement using infrared, ultrasonic, microwave, and similar technology. Data is collected and connected with other networks to evaluate and provide insight into the use of workplaces, making them an integral part of the IoT software.

2) **Smart Lighting:** Smart lighting is often the first step in modernizing office environment. According to Gartner, smart lighting has the potential to reduce energy costs by 90%. There are five key features of smart lighting: LED lighting, IoT sensors and controls, networking, analytics, and intelligence. IoT sensors detect motion in a room and turn on or off the lights accordingly. Lighting luminance controls change the lighting levels in spaces automatically relative to the daylight level available. The next generation of smart lighting is fully connected and puts even more control in the hands of consumers who can switch off and on the lights, monitor the lighting brightness and even change the color of smartphones.

3) **Smart Conference Room:** The smart conference room includes a variety of smart features to streamline and improve the employee meeting process. A meeting management system monitors use of common office spaces such as meeting rooms, hot desks, telephone booths, and huddle spaces. It speeds up the booking process for these spaces by cataloging each room in an online booking system that allows users to search and reserve spaces based on size, occupancy, and room characteristics. In just a few clicks, users can find and book a room, then order any required add-ons from the same site, such as catering or A/V equipment. A meeting management system also manages appointments and alerts guests and administrators to any changes with time, venue, or cancellations.

4) **Smart Desks:** The smart conference room's siblings are smart chairs. Smart desks are searchable and bookable via an online booking system, similar to the smart conference room. A smart desk booking system not only helps employees find an available desk for the day, but keeps track of who has reserved every room, so that employees in the building can easily track colleagues (or not depending on their privacy mode). Many smart desk models also offer options for sitting or standing desks and recognize the needs of each client. The analytics of each desk breaks down the sitting and standing information of users and allow employees to compare their standing conduct against themselves or other employees. Sensor data also provides administrators with useful insight to consider the use and routine flow of traffic.

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

5) **Video Monitoring:** 2018 was the home security camera's year with emerging innovations like Ring and Sky Bell. Video surveillance provides the office with a level of security. It allows managers and supervisors collect data and assess the use of office spaces. Modern video screens have wide angle views, low lighting features, and impressive zoom characteristics. These often allow users to monitor multiple locations with split screen viewing and access from the smartphone or computer of a user at once. Photos are typically stored in the cloud and can be downloaded as necessary. These are easy to search by date and time.

6) **Indoor Way-finding:** The way the average smartphone user communicates with the world has transformed interactive maps and step-by-step directions. The same thing is happening inside the smart office halls. Employees and visitors of the indoor way-finding platforms let company navigate floor plans and find their way with their smartphones to points of interest within the office building [60]. It prohibits employees and office managers from acting as tour guides and keeps workers focused on their larger tasks. Only ask the worker sitting nearest to each floor's entrance and they're going to tell you their biggest disruption is being asked for directions every day.

7) **Time Saving:** Innovative technology solutions are provided by the smart office system to simplify complex tasks. These can be performed in a short time, allowing more meaningful work to be done by employees.

The modern office, shown in figure 1.1, continues to evolve. When new technologies emerge, they make our lives easier, safer, and more comfortable; these devices will not be long before they become regular office fixtures. Do you imagine working without an AC or an email in an office? Soon we're going to say the same about smart conference room systems and smart coffee machines.

Figure 1.1: Modern Office

History of Smart Office

The transition from the conventional to the new smart office workplace by dipping it into three phases:

Stages 1(1996-2006): That's the point at which everything began. To improve execution, use of tablets, cells and the Internet were carried out.

Stages 2(2006-2016): Innovations in programming have gotten modern. The coming of cell phones and other quick track gadgets into the market added to the innovation of utilizations, innovation and distributed computing.

Stages 3(2017 to date): Intelligent working environments are another wonder. Associations have a more noteworthy comprehension of the idea and consolidate robotized frameworks to make their workplaces super-productive, limit working expenses, and make a powerful and very much associated workplace for laborers too.

As per a report by Allied Market Research, the worldwide market for brilliant structures is projected to create at an accumulate yearly development pace of 29.5 percent somewhere in the range of 2012 and 2020.

Presently a day's, individuals are getting more subject to their compact gadgets like PDAs, PDAs and other scaled down gadgets. A huge number of convenient gadget clients are reliant that can be appeared on the PDAs, advanced mobile phones and numerous other smaller than normal gadgets. Special and most recent capacities are accessible to abet the advanced cell social orders in pervasive computing region; the remote highlights of convenient gadgets reenacted present day age of move-capacity. While giving outcome data, the pervasive gadgets can whimsically work in peripatetic environment which is named as the 'Pervasive Ad-hoc Network'. However, the cell phones have numerous shortcomings and some of them can be improved.

The Internet of Things (IoT) has developed principally from omnipresent computing. While there is almost no qualification in certain contentions, IoT is probably going to be more in accordance with omnipresent computing than the first perspective on pervasive computing by Weiser.

Like pervasive computing, IoT-associated gadgets convey and give notices about use. The vision of universal calculation in regular articles is computing power that is generally spread in everyday life. The IoT is headed to convey this fantasy and change regular articles into associated gadgets. However, as of now, it requires a great deal of arrangement

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

and human connection—something that Weiser's pervasive innovation doesn't.

IoT (Internet of Things)

IoT is the ever-growing network of physical objects with an Internet connectivity IP address and interaction between these objects and other Internet-enabled devices and systems. IoT goes on to say that Internet connectivity extends beyond typical apps. To a variety of devices and everyday things that use embedded software to connect and interact with the outside world, all through the Internet. Pervasive computing and IoT examine similar problems and face similar challenges.

IoT is an innovation in which devices are coordinated with the virtual universe of the Internet and collaborate with it by tracking, sensing and monitoring objects to communicate with each other. An integrated architecture for smart campus towards the IoT is proposed on this study focused on the ZigBee wireless sensor network. IoT is not involved in origin, but in its execution it is intricate. Each single part is clear, but IOT needs several fragments. There are various IoT platform components such as sensors, power source, control unit, and design of interaction. The interaction module is the device component that supervises the device's correspondence with the IoT stage in order to exchange data between them. The features of a device that can act as a member of an IoT network are summarized as follows:

Sensors are a system that senses and responds to some kind of feedback from the physical environment. The data could be light, cold, moving, humidity, weight, or any of an incredible number of other natural wonders.

An actuator is a device that converts energy into a controlled movement. An actuator includes an energy source and a control signal. Typically it is used to apply a force to something.

IoT Gateway is a tool that fills in as the point of connection between IoT and cloud devices. This gateway may be a digital or hardware device.

Mobile Computing

Versatile computing is an interface among people and machines through which a PC should be shipped during normal use. The appearance of "portable computing" has denoted another period in correspondence and data framework. Programming empowers information to be sent through a gadget without interfacing with a fixed actual association. It is simpler to catch or listen in on correspondence channels since remote correspondence happens basically through radio signals instead of wires. Thusly, from every one of these dangers, it is important to give assurance. Security issues of

different sorts, like protection, trustworthiness, openness, validity and straightforwardness, should be tended to separately. In field of media communications, there is a genuine transformation over the most recent couple of years. Notwithstanding the three ages of remote cell frameworks, ubiquitous computing was conceivable because of advances in remote correspondence innovation and the accessibility of various lightweight, minimized, convenient computing gadgets like workstations, PDAs, cell phones and electronic coordinators.

LITERATURE SURVEY

PERVASIVE COMPUTING

Pervasive computing is an arising field with new advancements expecting to improve the proficiency and unwavering quality of the framework. Hennessy et al (2003) talks about asset the board for a start to finish pervasive computing environment. The paper features central models of asset the board, asset situated programming language highlights and static examination and arrangement procedures for outsider asset utilization. A concise portrayal is likewise made about the significance of trust and notoriety in the field of pervasive computing, which is consistently unique in nature.

Pervasive computing guarantees a hugely organized world supporting a populace of assorted yet agreeable portable elements. It has highlights, for example, (I) accessibility of incomplete data accessible (ii) obscure purchasers because of their portability and unpredictability (iii) need focal control due to likely being (iv) separation from its home organizations (v) Intelligent detecting with savvy detecting substances. These sorts of versatility, vulnerability and heterogeneity make trust the board more muddled. Much of the time, a unique trust the board, explicitly trust foundation, is required for cooperation among these substances. A trust model for this reason ought to be intended to be adaptable and versatile. Pervasive computing environments center around incorporating computing and correspondence advances with the encompassing actual environment to improve on everyday client exercises (Black et al 2004).

Sathyanarayanan (2001) has examined about the difficulties in PC frameworks research presented by the arising field of pervasive computing. He looks at the relationship of this new field to its archetypes: circulated frameworks and portable computing and afterward distinguishes four new examination pushes: successful utilization of brilliant spaces, imperceptibility, confined adaptability, and concealing lopsided molding. Then, it several

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

speculative pervasive computing situations, and utilizations them to distinguish key abilities that are absent from the present frameworks.

In pervasive computing, various, nonchalantly available, frequently undetectable, versatile or installed gadgets are associated with an undeniably pervasive organization design and gather data about the general environment of pervasive computing utilizing sensors (Denko et al 2008). Pervasive computing can be utilized in various applications, like medical clinics, savvy homerooms, building destinations, arenas, shopping centers, crisis administrations, conference halls, combat zones, and unfriendly actual environments. Inside remote organizations, there exists a subcategory, which includes impermanent, and dynamic organizations whose creation changes habitually. These environments, called specially appointed organizations, present extraordinary difficulties to designers, chairmen and clients.

The remote specially appointed organizations have been additionally separated into "oversaw impromptu organizations" and "Unadulterated specially appointed organizations", as per Ranganathan (2004). Overseen specially appointed organizations include circumstances where suspicions can be made with respect to the arrangement environment and the presence of different elements. In these circumstances, a manager can use this data before organization. "Unadulterated impromptu" environments comprise of circumstances where no information on the organization environment is expected. These organizations require no pre-design and as a rule hold all elements equivalent.

SECURITY AND PRIVACY APPROACHES IN WSN

Security may be a widely used term, together with the attributes of integrity, authentication, non-repudiation, privacy and anti-replay. Depending on the network information, it provides a larger threat of transmitting secure information over the network. It is used for the safe transmission of various well-known technologies. This section describes network security technologies and wireless networks.

CRYPTOGRAPHY APPROACHES

Encryption-decoding innovation, intended for customary wired organizations, which can't be practically open to remote organizations. The WSN comprises of little hubs with absence of handling, memory, and force. All cryptographic plans require additional digit move and require extra preparing, memory, and force, which are the basic assets for sensor life. Applying security strategies, for example, increment delay in encryption, jitter and parcel disappointment in remote organizations. Likewise, when it applies a cryptographic plan to a WSNs, there are various significant issues, for example, how keys are created or spread, taken care of,

annihilated, or relegated to new sensors added to the organization, or how keys are restored to guarantee the solid security of the organization. Since cooperation with people at any rate is the fundamental capacity of a remote organization, the way to adjust the key for encryption is a significant issue. The appropriation of pre-stacked keys or inserted keys, can't be equipped for being a compelling clarification.

KEY MANAGEMENT APPROACHES

Because of the personality of remote organizations, a great deal of set up key administration approaches in existing remote organizations can't be reasonable on to remote organizations. In remote organization security arrangements, encoding innovation is the reason for a scope of security advancements by scrambling remote organizations which will address issues like validation, privacy, non-renouncement, and respectability. For encoding innovation, center administration ought to act naturally tended to. In flow years, specialists recommended various key administration frameworks. The code framework unintegrated into respective and lopsided key administration frameworks. Retribution on the key assignment method of the hub, it could be separated into the self-assertive key administration framework and deterministic key administration framework. Circulated key administration approach and progressive key administration approach might be ordered per geography.

Symmetric and Asymmetric Approaches: Depending on an assortment of encryption framework to oversee remote organizations that can be isolated into the control and the executives of symmetric and unbalanced key. In symmetric key administration, the encryption and unscrambling keys of the sensor hubs are something very similar, basic, computational and capacity less, when contrasted with uneven keys. Symmetric keys profit by computational intricacy however is insufficient for key administration and security. Uneven key administration is considered improper for remote organizations because of the appeal for PC related capacities, stockpiling, and correspondence hubs. Be that as it may, because of the progressive expansion in related examination, a portion of the lopsided encryption calculations would now be able to be applied to remote organizations.

Bauer and Lee et al.[37] proposed an authentication protocol by means of the appearance of an undeclared contribution and encryption group. The network grid consists of multiple subsets of the network. Each subset contains a base station and the subgroups correspond to each other by a base station. Software optimization does not use the prominent use of the encryption/decryption program in the authentication process except utilizes an unknown

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

scheme for sharing and collective agreement, and tolerance for the shortage is higher; it is computationally efficient and has high authentication power. The drawback of the program is that the entire nodes in the subset must cooperate collaboratively upon authentication. Conflicts of information can occur when the node offers a specific packet.

Watro et al.[38] proposed TinyPK entity authentication supported on the RSA algorithm. The TinyPK Authentication Protocol can use a dispute respond method to authenticate external institutes and safely transfer session keys to third parties in the wireless network. This program utilizes a low-index RSA algorithm that reduces load and storage in some coverage. On the other hand, it designed a protocol that allows the common node to encrypt data consumption of small and small resources and sign checks and perform large-scale decoding and power consumption for signing so that the program can be applied only to limited sensor resources devices. They are carried out by workshops or peripheral assemblies with energy. However, this system security is not high. If the node is held by authentication, the complete network becomes insecure, and if the key length is too extensive, the arithmetic overload becomes large.

Ouadjaout et al.[39] recommend SMRP, a multi-path RT-Protocol and, based on the SEIF plan. In this SEIF plan, the wireless network control node and sends a key update command for each specific slot. When it receives a regular node update key command, it updates the key and reports the updated results to the control nodes in its system. The dominant node is the correct node that did not update its own key in time to be a captive node and sends an unacceptable broadcast in the cluster. As a consequence, the "SELF" able to use the sensor holding keys that were captured to avoid impersonating the enemy as a legitimate node.

Filip Perich et al. (2006) [68] puts light on versatile information the executives, regularly dependent on the worker/intermediary/customer model. In Information and Communications Technology (ICT) new time, cell phones have become both information customers and makers. The creator depicts the new information the executives challenges through a model of the structure, MoGATU, which tends to versatile information the board difficulties. A significant segment of the methodology is to regard every gadget as a self-ruling element with its "objectives" and "convictions", communicated utilizing a semantically rich language. The creator has carried out this system over a joined Bluetooth and Ad-Hoc 802.11 organization with customers running on an assortment of cell phones.

Munirul Haque et al. (2006) [74] depicts security in ubiquitous computing the current status and open issues. A huge number of clients of remote gadgets are ever progressing, progressively subject to their

PDAs, advanced cells, and other handheld gadgets. Such gadgets' portable presence has encouraged another period of adaptability. Many such gadgets can enter and leave an organization haphazardly, establishing a roaming environment known as a ubiquitous specially appointed organization. In any case, there are intrinsic blemishes in cell phones. The main issue is security in ubiquitous computing. Security is needed to guarantee exact privacy, respectability, validation and control of access; to give some examples. Security research is ascending at this basic crossroads.

Long Zhao hua et al. (2010) [77] presents hypothesis of ubiquitous computing and its security issues. A structure for access control is executed by carrying out Tri-Element Peer Authentication (TePA) security system. It is like the security component of TePA and ideal for universal computing usefulness. It is agreeable with the current security systems and addresses explicit necessities of universal computing. Setting up secure correspondence depends on common trust. Various applications and setting require diverse level of trust in the universal computing environment. So it requires a quick and solid instrument to set up shared trust. This work proposes a security component like TePA, and the framework is ideal for conveying universal computing administrations in remote LAN and furthermore improves their security and appropriateness.

RESEARCH METHODOLOGY

In this part, we show what the field of HCI (Human Computer Interaction) and related regions needs to introduce as far as planning PC frameworks. In the first place, we state one of the essential perspectives on Human Computer Interaction plan for a particular client, playing out a particular errand, in a particular area. As we go to clarify an assortment of advancements, activities, strategies and approaches, we remember these three measurements: client, assignment and area.

We proceed with the study by finishing a fundamental lifecycle of data: first, data should be produced, at that point dispersed, and afterward introduced for correspondence with the client. For every one of these stages, we exhibit work that is related to the plan and execution of PC frameworks and specifically pervasive PC frameworks. Since the last is another field inside Computer Science, the total store of frameworks configuration has not yet been attempted and applied to pervasive frameworks. Consequently, it very well may be significant to learn plan techniques that have been applied else-where, despite the fact that they are not of straight connection to the plan of pervasive frameworks.

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

Having reviewed different plan approaches, structures and executions, we at that point returned to HCI. We have shown that, considering our overview of configuration issues and pervasive computing, the regular HCI approach of client - task - space is inadequate. In this part we depict the methodology, as a structure for planning pervasive frameworks.

ANALYSIS OF RESULTS

In this section, we do test and examine the aftereffect of the proposed framework in a clinic the executive's framework.

We apply the stockpile at a more elevated level than in the past section. We show how the plan apparatus can be applied post hoc to clarify issues that have effectively been recognized in a genuine setting. Moreover, we utilize the plan device to propose another framework and deduced distinguish likely issues with it.

The setting we tackle is the Accident and Emergency office in Government Hospital, India. To do this, we have utilized material gathered during a multi month actual investigation of this medical clinic. The hands on work study itself, announced zeroed in on recognizing methods of giving better data assets to the medical clinic patients. As a rule, the shortfall of this data had adverse consequences, including brutality and attacks. In this examination study we transform the hands on work discoveries and proposition into plan arrangements.

Viciousness and maltreatment towards clinic staff should be sufficiently wide - spread and genuine to require the new declaration by the Indian Government of new public rules to help make clinics more secure environments for both staff and patients. Clinics are presently permitted first to caution and afterward to reject without treatment patients or guests who are vicious or oppressive. In spite of such measures, the issue is apparently still on the increment, and is by all accounts especially common in Emergency divisions. A few occurrences were noticed or announced during the hands on work. Most of these episodes included impoliteness or obnoxious attack of staff and different patients. Nonetheless, even patients whose conduct didn't drop to these levels were consistently seen to give indications of aggravation, stress and irritation, and these responses would in general concur with significant delays.

CONCLUSION

We tended to the plan of pervasive frameworks on three discrete levels, every one of which has various necessities. We did this by applying the plan thoughts to interface level plan (with the plan of an association strategy), plan investigation and assessment in the crisis office. The way that the thoughts were appropriate to shifting levels of investigation is an empowering marker for us. At last, it is important that the thoughts introduced in this work relate basically to the constructed environment and to industrialized social orders with a high infiltration of computing assets and abundance. To plan really pervasive frameworks in the most flawless worldwide sense will require significant changes in political, conservative, social and innovative turn of events. A structure and configuration devices for a particularly worldwide framework stays a test. The difficulties confronting pervasive computing are extraordinary, yet its objective is significantly more noteworthy. We firmly accept that society can profit from various perspectives from this sort of innovation, and we additionally accept that progress inside this space ought to be founded on solid hypothetical grounds.

REFERENCES

[1]   Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang (2002), "A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Network," Proc. Eighth ACM Ann. Conf. Mobile Computing and Networking, pp. 148-159.

[2]   Soroush, M. Salajegheh, and T. Dimitriou (2007), "Providing Transparent Security services to Sensor Networks," in Communications, ICC'07, IEEE International Conference on, Glasgow, pp. 3431-3436.

[3]   S. Zhong, J. Chen, and Y. R. Yang (2003), "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks", in Proceedings of IEEE Infocom '03, San Francisco, CA.

[4]   S. Marti, T. J. Giuli, K. Lai, and M. Baker (2000), "Mitigating routing misbehaviour in mobile ad-hoc networks", in Mobile Computing and Networking, pp. 255-265.

[5]   Chang and H. C. Tsai (2010), "An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks", IEEE Trans. on Wireless Com., vol. 9, no. 11, pp. 33.

[6]   Chhabra, B. Gupta and A. Almomani (2013), "A Novel Solution to Handle DDOS Attack in MANET", Journal of Information Security, 4(03), pp. 165-179. doi:10.4236/jis.2013.43019.

[7]   Chan, A. Perrig, and D. Song (2003), "Random key predistribution schemes for

Bhawna Kaushik[1]* Dr. Ali Akbar Babalal Bagwan[2]

sensor networks", in Proceedings of the IEEE Symposium on Security and Privacy, pp. 197-213, Washington, DC, USA.

[8]   X. J. Du, M. Guizani, Y. Xiao and H. H. Chen (2009), "Transactions papers a routine-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks", IEEE Transactions on Wireless Communications, vol.8, no.3, pp. 1223-1229.

[9]   Y. Qiu, J. Y. Zhou and J. Baek (2010), "Authentication and key establishment in dynamic wireless sensor networks", Sensors, vol. 10, no. 4, pp. 3718-3731.

[10]   W. Shi and P. Gong (2013), "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography", International Journal of Distributed Sensor Networks.

Corresponding Author

Bhawna Kaushik*

PhD Student, Kalinga University, Raipur