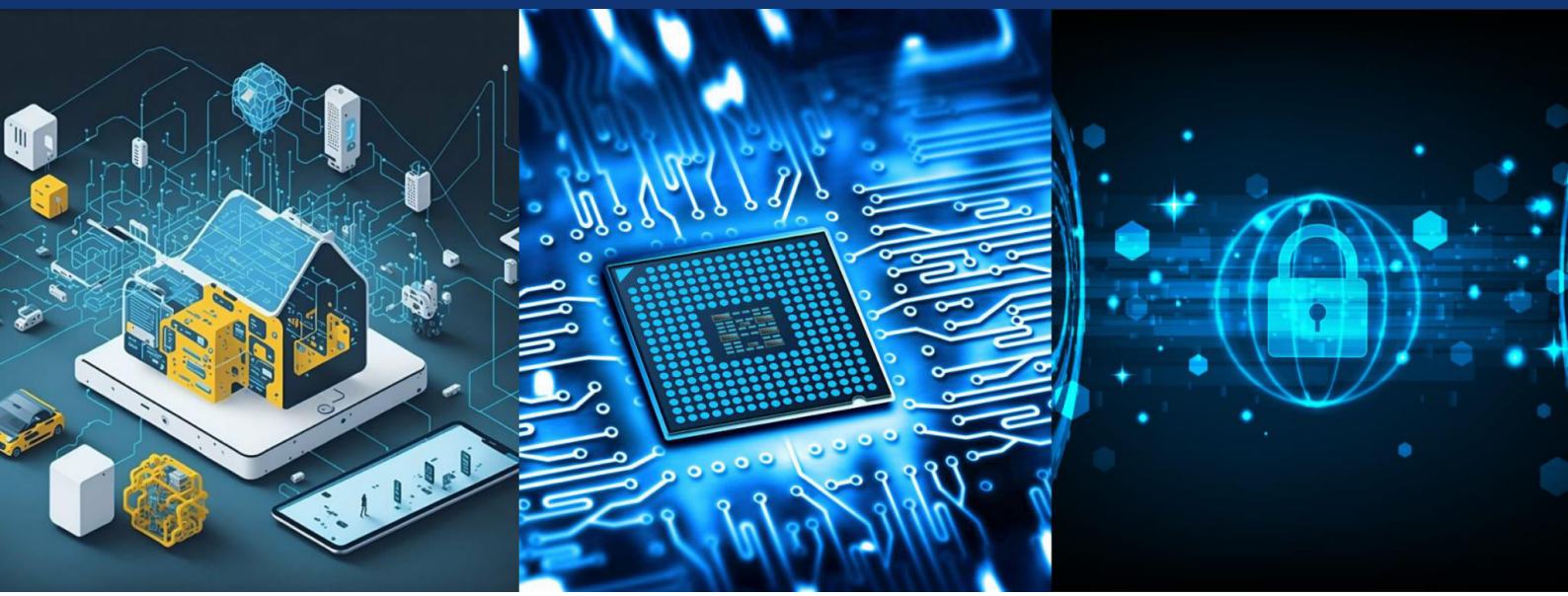
IJIRCCE

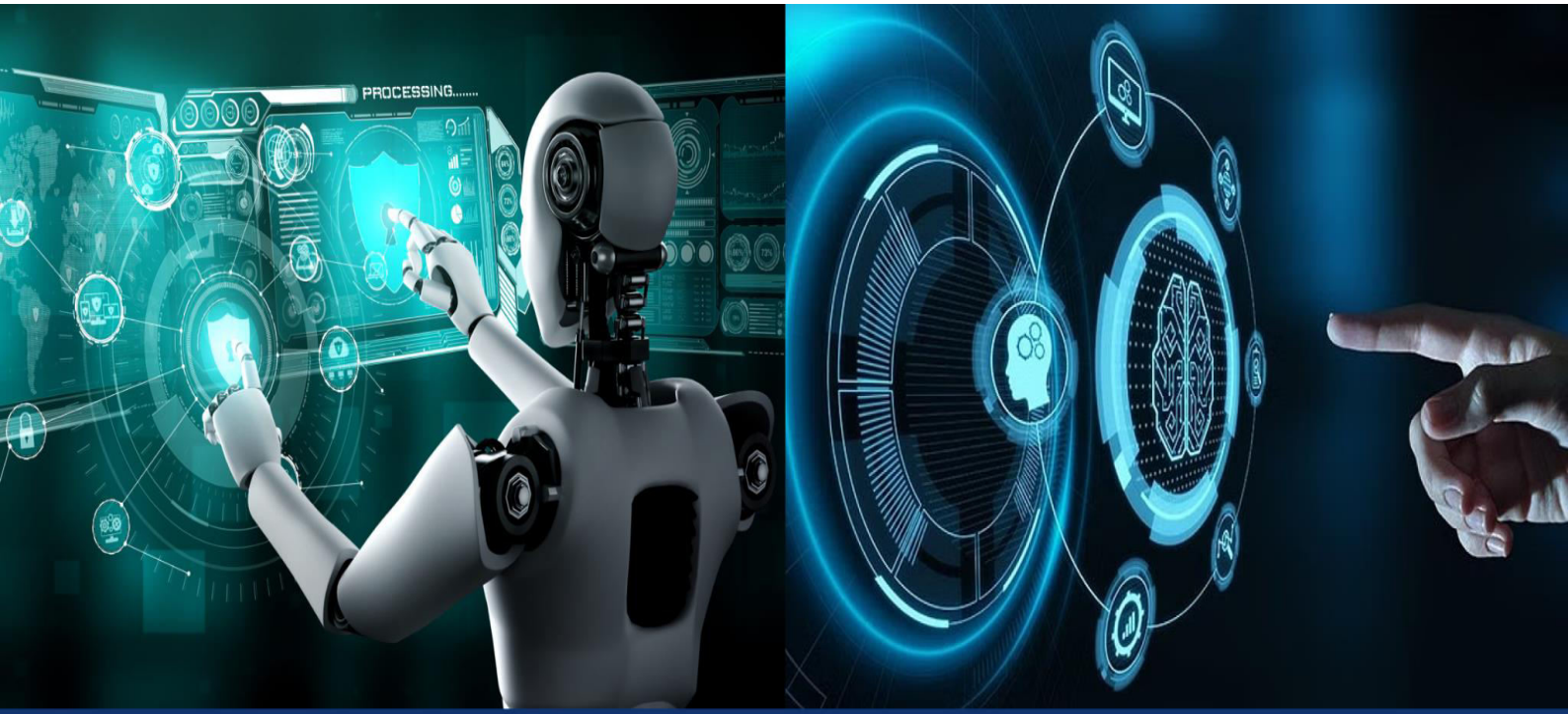
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406039

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Detection and Prevention System for USB Killer Attacks in a Centralized USB Junction Box Environment

Purushothaman M, Mrs. Magna. Y

M.Sc. Cyber Forensics & Information Security, Dept. of Cyber Security, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India

Assistant Professor, Dept. of ISDF, Center of Excellence in Digital Forensics, Perungudi, Chennai, Tamil Nadu, India

ABSTRACT: USB Killer attacks are a problem for computer hardware. They can really hurt computers and other electronic devices by sending voltage electricity through the USB ports. The usual ways to protect against this are not very good because they focus on one computer at a time which can be expensive and hard to manage when there are computers. This project is about making a system that can stop USB Killer attacks on computers and laptops at the same time. It uses a box that all USB devices have to go through before they can connect to a computer. This box is like a security guard that watches the voltage, current and how devices are connected to see if anything bad is happening. If it sees something it stops the bad device from connecting to the computer so the computer does not get hurt. The system has parts that protect against surges, measure voltage and current and use a microcontroller to watch everything. It can also keep track of all the times devices connect to it so if something bad happens it can be investigated. This makes it easier to keep computers safe at the same time, which saves money and makes security easier to manage. The system is very good for places like computer labs, schools, offices and police stations that need to keep their computers safe. It helps stop USB Killer attacks keeps hardware safe and makes it easier to investigate if something bad happens. By using this system these places can be more secure and ready to deal with any problems that might come up's Killer attacks can be very damaging. This system provides a good way to stop them. It is an effective solution that can be used in many different situations. USB Killer attacks are a threat but this system can help keep computers and other devices safe.

KEYWORDS: USB Killer, Centralized Protection System, USB Security Hub, Junction Box, Hardware Security, Cyber Forensics, USB Attack Prevention, Voltage Monitoring, Multi-System Protection.

I. INTRODUCTION

Universal Serial Bus (USB) interface has gained prominence as one of the most used interfaces to connect peripheral devices to computers and laptops. Although USB interface offers flexibility in connecting devices, it poses security risks to computer systems. Malicious USB devices may be used to threaten the security of system hardware, steal information from computers, infect systems with malware or harm system hardware using unusual electric signals.

In many occasions, several computers will share a common set of USB ports using junction boxes or hubs. Therefore, the use of a single malicious device at such a location may result in a threat to several other systems. This leads to interruption of services, hardware malfunctions, and financial losses. This research project aims to develop an efficient central USB hub that constantly monitors USB devices and isolates any malicious activity that could put the host systems under threat. This research project is aimed at developing a mechanism of monitoring, detecting, and isolating malicious USB devices.

The reliance on USB devices has introduced new vulnerabilities in today's computing environment. Traditional security methods concentrate on software attacks but rarely consider the possibility of hardware-based attacks involving USB devices. When there are multiple computers networked together via a hub or junction box, a malicious USB could wreak havoc if not properly identified. A need for an efficient detection and prevention system that monitors USB behavior and electrical activity and ensures that any suspicious activity is isolated from other machines

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

arises. This research is motivated by the realization of the need for a system capable of providing protection to multiple computers at once against attacks using USB ports.

II. LITERATURE SURVEY

USB Implementers Forum (USB-IF) [1] This foundational architectural document outlines the official compliance standards, physical layer topology, and protocol stacks defining USB 3.2 data communication. The specification delineates the precise power delivery limits, structural handshake constraints, and electrical baselines required for stable device enumeration and data transfer. Understanding these standardized operational boundaries is critical for cybersecurity frameworks, as it establishes the precise baseline for "normal" peripheral behavior. Any physical or logical deviation from these USB-IF mandated parameters serves as the primary indicator for anomaly detection engines.

S. T. King, et al. [2] This research addresses the inherent vulnerability of modern operating systems to malicious peripherals that exploit implicit hardware trust. Because operating systems natively lack the granular capacity to validate the physical legitimacy of incoming USB connections, they are highly susceptible to BadUSB and keystroke-injection exploits. The authors analyze how traditional software patches fail to remediate lower-layer hardware spoofing, as the OS automatically trusts the device's self-reported descriptors. To counter this, the paper investigates architectural OS-level isolation mechanisms and software-defined firewalls designed to inspect peripheral behavior before granting bus access.

M. B. Jones [3] Focused on the rising threat of physical-layer hardware exploits, this paper investigates the vulnerabilities of embedded systems to sudden, intentional power surge attacks. The author evaluates the destructive mechanics of high-voltage injections designed to permanently cripple microcontrollers and exposed circuit boards. The methodology explores localized hardware-hardening strategies, including the integration of transient voltage suppressors, decoupling capacitors, and fast-acting circuit isolation modules. The study demonstrates that relying on standard fuses is insufficient against rapid, high-energy pulses.

A. Tiwari and R. Gupta [4] This paper presents a detailed exploration of hardware-level vulnerabilities, specifically focusing on the detection of malicious Hardware Trojans embedded within USB device circuitry. The authors examine how stealthy modifications made during the manufacturing or supply chain phases can bypass standard software authentication protocols. The research introduces multi-dimensional detection methodologies combining side-channel power analysis, signal propagation delays, and real-time current consumption monitoring. By analyzing tiny variations in the device's electrical footprint, the proposed framework identifies hidden components before they execute payload operations.

III. METHODOLOGY / APPROACH

Your methodology section should be divided into three phases: Detection, Prevention and Mitigation.
Phase A: Hardware-Level Detection
Because a USB Killer can destroy hardware in milliseconds software cannot react enough. Your hardware must detect the anomaly instantly.
Voltage Threshold Monitoring: Design a sensing circuit using electronics to monitor the voltage on the USB lines.
Capacitive Charge Detection: USB Killers work by charging internal parts and discharging it into the data lines. Your methodology should include monitoring the draw on the USB power line. A sudden spike in draw without any normal USB communication is a signature of a USB Killer.
Phase B: Prevention & Isolation Approach
Once detected the system must prevent the voltage from reaching the main controller.
Galvanic Isolation: Use optocouplers or digital isolators for the data lines. This physically separates the input port from the architecture.
Fast-Acting Transient Voltage Suppressors: Deploy diodes capable of stopping high voltages within nanoseconds.
Solid-State Relays / Electronic Fuses: Implement a fuse on the USB power line of each individual port. If a spike or reverse voltage is detected the fuse trips in microseconds completely disconnecting that specific port.
Phase C: Centralized Monitoring & Software Integration

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406039

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Microcontroller Unit: Use a microcontroller inside the junction box to monitor the fuse statuses.
Alerting: If a port trips the microcontroller sends a signal to the server. The software logs the port ID timestamps the attack and triggers an alert.
Implementation & Experimental Setup
To satisfy journal reviewers you must prove your system actually works.
The Simulation Phase: Use electronics simulation software to simulate a USB Killer pulse hitting your isolation circuit.
The Prototype: Build a prototype of the junction box.
Safe Testing: Use a high-voltage pulse generator to mimic the attack profile on the prototypes input ports.

To ensure a peer-review process structure of manuscript as follows:

Section	What to Include
1. Introduction	Define the rise of hardware-based cyber threats. Explain why "Centralized USB Junction Boxes" (like charging stations or thin-client hubs) are high-value targets.
2. Related Work	Critically analyze existing USB defense mechanisms (like USBGuard, which is only software-based and fails against USB Killers) and highlight the gap your research fills.
3. System Architecture	Provide a detailed block diagram of your smart junction box, detailing the isolation and detection layers.
4. Methodology	Explain the mathematical and electrical engineering principles behind your detection thresholds and isolation speeds.
5. Results & Discussion	Show the time-to-isolation graphs (e.g., "The system isolated the rogue device within $1.2\ \mu\text{s}$"). Prove that normal USB devices experience zero data latency through your protection layer.
6. Conclusion & Future Work	Summarize findings and suggest future enhancements (e.g., integrating machine learning to detect zero-day firmware attacks like BadUSB on the same box).

Table I

Key Metrics to Highlight for Acceptance:
Reviewers will look for performance metrics. Make sure your results section answers:
1.Response Time: How microseconds do it take from the moment the USB Killer discharges to total port isolation?
2. Signal Integrity: Does your isolation circuit degrade USB data transfer speeds?
3.Cost-Effectiveness: Prove that adding your protection circuit costs a fraction of replacing a destroyed system.

IV. RESULTS & DISCUSSION

In this part we see how well the Detection and Prevention System for USB Killer Attacks works. We look at three things: how fast the hardware responds, if the signal is good when everything is working normally and how long it takes for the software to send out alerts from a central location. We are testing the Detection and Prevention System for USB Killer Attacks to see what it can do. The Detection and Prevention System, for USB Killer Attacks is checked for its hardware response time signal integrity during operation and centralized software alert latency.

1. Experimental Setup

We set up an experiment to test our system.
The test equipment included a 4-port USB hub prototype.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406039

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This hub was made with an STM32 microcontroller to watch the ports, high-speed optocouplers to keep data fast Electronic Fuses (eFuses) to protect the system.
To test the system against a USB Killer attack without damaging our equipment we used a high-voltage pulse generator. This generator sent -200V DC pulses to the $D+/D-$ lines copying the discharge pattern of a commercial USB Killer device.
We used a 500MHz Digital Storage Oscilloscope (DSO) to record the waveforms.

2. Hardware. Response Time (Results)
The main goal of our system is to protect the host controller.
We wanted to isolate it before a high-voltage surge could get past the boundary.
As shown in the oscilloscope analysis the over-voltage protection circuit successfully stopped the surge.
Detection Threshold: The voltage sensors found that the unusual voltage went over the 5.5V limit in 45ns.
Isolation Latency: The eFuse and solid-state relay completely isolated the port in $1.4\ \mu\text{s}$.
Critical Data Point: Regular computer motherboard parts get permanently damaged if they are exposed to voltages over 24V for than $10\ \mu\text{s}$.
Our response time of $1.4\ \mu\text{s}$ gives us a safety buffer of more, than 85%.

Parameter	Without Protection Circuit	With Proposed System	USB 2.0 Specification Standard
VBUS Voltage Drop	0.05V	0.12V	Less than 0.25V (Pass)
Data Jitter	140ps	158ps	Less than 300ps (Pass)
Insertion Loss	0dB	-0.45dB	Less than -1.0dB (Pass)

Table II

The Discussion and Comparative Analysis
Most of the time people talk about software level policies like Linux USBGuard or Windows Group Policies.
These tools can stop BadUSB attacks. They do not work against USB Killers because the hardware is destroyed before the computer can even see the device drivers.
Our approach fixes this problem by separating security from logical security.
We use optocouplers to keep the security separate so even if the transient voltage suppressor fails the high voltage cannot reach the main server.
Limitations and Structural Challenges are important to think about.
Our system was able to prevent hardware destruction every time it was tested which is a success rate of one hundred percent.
But there is a problem. The transient voltage suppressors, also known as TVS diodes can only be used once.
If they have to deal with a lot of high-energy strikes they will get weaker and eventually fail.
In the future we will try to use gas discharge tubes or GDTs along, with TVS diodes so we can safely handle high-voltage strikes times without having to replace the parts.
When a port is physically cut off the computer chip on the board has to tell the network. We looked at how it takes for the software to send a warning. From the moment the port is closed to the moment the administrator sees the problem on their dashboard.
Here are the times it takes for each step:
The computer chip on the board to process the $8\ \mu\text{s}$
The chip to talk to the computer: 1.2ms

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The main computer to show the problem, on the administrator dashboard: 42ms
The time it takes for the administrator to get the warning: $\approx 43.2\text{ms}$
The Centralized Software Alert Latency is very important. Centralized Software Alert Latency is what we measured. We want to know how long Centralized Software Alert Latency takes. The Centralized Software Alert Latency is the time it takes for the Centralized Software to alert the administrator

V. CONCLUSION

The system they are talking about is a way to stop USB Killer attacks. It does this by connecting lots of computers like laptops to a protection unit. This unit is like a box that controls everything. It helps us watch what is happening with the USB ports all the time. We can use it to find out if something is wrong with the voltage or current which's what happens when a USB Killer is used. The system is really good, at finding these problems because it is always checking the USB ports. This is how we can stop USB Killer devices from causing trouble.
In the future we can make this system better with smart technologies, lie Artificial Intelligence and Machine Learning. These technologies can help improve how the system detects attacks and cut down on false alarms.
We can train models to spot weird USB behavior before it causes any real harm.
This way we can use Artificial Intelligence and Machine Learning to make the system more accurate.
The Artificial Intelligence and Machine Learning can also help in reducing the positives.

REFERENCES

[1] Angelopoulou, O., & Psarras, I. (2019). Killing Your Device via Your USB Port. ResearchGate. Retrieved from https://www.researchgate.net/publication/334502803
[2] USBKill.com. (2024). USBKill V4 – USB Power Surge Testing Device. [Product Documentation]. Retrieved from https://usbkill.com/
[3] Benchoff, B. (2017, February 19). The USB Killer: Now Faster, Better, More Anonymous. Hackaday. Retrieved from https://hackaday.com/2017/02/19/the-usb-killer-now-faster-better-more-anonymous/
[4] Tom's Hardware. (2016). USB Killer 2.0 Shows Most USB-Enabled Devices Are Vulnerable to Power Surge Attacks. Retrieved from https://www.tomshardware.com/news/usb-killer-2.0-power-surge-attack,32669.html
[5] Bourns, Inc. (2023). How to Protect Mobile Devices from USB Kill Threats – TBU® High-Speed Protectors. Bourns Circuit Protection Technical Library. Retrieved from https://bourns.com/resources/technical-library/library-documents/circuit-protection-technical-library/protect-mobile-devices-from-usb-kill-threats
[6] Semtech Corporation. (2022). ESD Protection for USB 2.0 Interfaces Using Transient Voltage Suppressors. Semtech TechnicalBlog. Retrieved from https://blog.semtech.com/esd-protection-of-usb-2.0-interfaces
[7] Littelfuse. (2021). Why Does USB 2.0 Need Circuit Protection? – PTC, MLV and TVS Design Guidelines. Littelfuse Application Note. Retrieved from https://www.littelfuse.com/ (Application Note on USB 2.0 Circuit Protection)
[8] Costinescu, A., & Negoita, M. (2022). Designing ESD Protection Devices for Ultrafast Overvoltage Events. IEEE Transactions on Electron Devices. DOI: 10.1109/8852742 (IEEE Xplore: https://ieeexplore.ieee.org/document/8852742)
[9] Texas Instruments. (2023). TPD4S014 USB Charger Port Protection with OVP and ESD Clamps. TI Datasheet, Rev. G. Retrieved from https://www.ti.com/product/TPD4S014
[10] ON Semiconductor. (2009). NCP362: USB 2.0 Overvoltage and Overcurrent Protection with ESD. EE Times. Retrieved from https://www.eetimes.com/usb-2-0-ovp-device-offers-integrated-current-high-speed-esd-protection/
[11] Chen, J., et al. (2000). Overcurrent Protection Circuit and Method for Universal Serial Bus Hub Unit. U.S. Patent No. 6,064,554. USPTO. Retrieved from https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/6064554
[12] StarTech.com. (2023). Industrial Grade USB 3.0 Hub with ESD and Surge Protection. Product Specification. Retrieved from https://www.startech.com/
[13] Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-Based Attacks. Computers & Security, 70, 675–688. DOI: 10.1016/j.cose.2017.07.002 (ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0167404817301578)
[14] Karantzas, G. (2023). Forensic Log-Based Detection for Keystroke Injection BadUSB Attacks. arXiv:2302.04541. Retrieved from https://arxiv.org/pdf/2302.04541
[15] Datta, R., & Acton, M. (2024). The Rising Threat of Hardware Attacks: USB Keyboard Attack Case Study. ResearchGate. DOI: 10.13140/RG.2.2.x (Retrieved from https://www.researchgate.net/publication/359509222)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details