Towards an IoT Community-Cluster Model for Burglar Intrusion Detection and Real-Time Reporting in Smart Homes

Ryan Singh[1], Haider Al-Khateeb [1,*], Gabriela Ahmadi-Assalemi[1], and Gregory Epiphaniou[2]

[1] Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, UK
[2] University of Warwick, WMG Group, Coventry, West Midlands, UK

[*] Corresponding Author: H.Al-Khateeb@wlv.ac.uk

Abstract. The systematic integration of the Internet of Things (IoT) into the supply chain creates opportunities for automation in smart homes from concept to practice. Our research shows that residential burglary remains a problem. Despite the paradigm shift in ubiquitous computing, the maturity of the physical security controls integrating IoT in residential physical security measures such as burglar alarm systems within smart homes is weak. Sensors utilised by burglar alarm systems aided by IoT enable real-time reporting capabilities and facilitate process automation which can be innovatively employed to increase security resilience and improve response to a burglary in smart homes. We research key-related methods of proposed security of home alarm systems and introduce an IoT Burglar Intrusion Detection (I-BID) solution, a new privacy-preserving alarms system with multi-recipient real-time reporting of intrusion in smart homes. Our approach is demonstrated on a developed and tested prototype artefact. The experimental results reveal that the proposed technique reliably detects intrusion, achieves real-time reporting of a home intrusion to multiple recipients autonomously and simultaneously with a high degree of accuracy. The key strength of our technique is its scalability to a community-cluster model as a burglary security mechanism.

Keywords: Internet of Things, monitor, detect, alert, police, incident response, intrusion, sensor, smart home, unauthorized access, burglary

R. Singh, H. M. Al-Khateeb, G. Ahmadi-Assalemi, and G. Epiphaniou "Towards an IoT Community-Cluster Model for Burglar Intrusion Detection and Real-Time Reporting in Smart Homes", in *Challenges in the IoT and Smart Environments, A Practitioners' Guide to Security*. *Advanced Sciences and Technologies for Security Applications*, R. Montasari et al., Ed. Cham: Springer International Publishing, 2021, pp. 53-73, Print ISBN: 978-3-030-87165-9, Electronic ISBN: 978-3-030-87166-6. DOI: doi.org/10.1007/978-3-030-87166-6_3. [online]. Available: https://doi.org/10.1007/978-3-030-87166-6_3

1 Introduction

The Internet of Things (IoT) is a novel paradigm integrating physical devices and sensors with digital capabilities of network technologies [1] creating new opportunities for performance and functionality enhancement. According to [2], IoT fused with the 5th generation mobile network's (5G) ubiquitous infrastructure is expected to have a "massive impact on society and business bringing about societal and economic opportunities for everyday connected objects and innovative applications across several smart sectors including smart homes". Although, according to [3] smart homes are in the earlier stages of development compared to other smart city sectors, safety-related applications in smart homes, are one of the forward-looking IoT driven innovations to help address problems in the physical security control realm.

Office of National Statistics (ONS) reporting shows that despite an overall decrease of 4% to 417,416 in burglary offences recorded by police across England and Wales (excluding Greater Manchester figures) in June 2019, of which 291,816 were categorised as residential burglary [4]. Although burglaries reported by the police showed a slight decrease as reported for the period ending in June 2019, these offences had shown a rise in recent year by 6% in the year ending March 2018 and 3% in March 2017 [4]. In the year ending September 2020, ONS reported a 20% drop in burglary compared with the previous reporting period, however, it is noteworthy that this drop is largely attributed to the lockdown restrictions and fluctuation in police recorded crime during this period [5], and residential burglary remains a problem. It is worth noting, that burglary is a crime considered to be well reported by the victims and well recorded by the police.

According to the ONS Crime Survey for England and Wales (CSEW) dataset [6] covering the period between March 2010 and March 2020, the dominant method of intrusion by criminals has consistently been the front door, followed by the back door, with crime prevalence during the week compared to the weekend and the evening or night period over mornings or afternoons with the dominant method of entry being forced locks. Apart from a monetary impact and damage to property, this type of crime considerably affects people in other ways including physically through the use of violence and emotionally [6], which is putting residents including vulnerable groups of people at additional risk.

Visible and audible home intruder alarms are considered a deterrent to a potential intruder. The traditional approach to home intruder alarms in the UK typically consists of audible, visible and remotely monitored alarms through an Alarm Receiving Centre (ARC) by a National Security Inspectorate (NSI) or Security Systems and Alarms Inspection Board (SSAIB) regulated provider. Depending on a plan, response varies from a keyholder only to combined with police response in the event of a confirmed alarm. The police response is governed by the National Police Chief's Council (NPCC) [7].

Standalone house alarms are not monitored by an ARC, therefore have no direct access to the police backed response. A final factor to consider is marginalised groups, examples include the rental market households require the agreement of the landlord and centrally maintained security systems can be potentially unaffordable for lower-income households.

The emerging concept of smart burglar alarm systems leverages IoT to address the problem of the traditional human-in-the-loop approach of intrusion detection in homes. In this article, the problem of physical security controls in smart homes is discussed alongside the concept of an IoT-based community-cluster model for physical security control in smart homes and real-time reporting in the prevalence of a detected intrusion. We discuss the key advancements in technology within homes and examine recent physical security protective systems. Furthermore, we present a system design, construct and evaluate a prototype artefact for a novel IoT based home security alarm system.

2 The Advancement of Digital Technology in Smart Homes Security

2.1 The Role of Transformational Technologies

IoT has evolved from the Radio Frequency Identification (RFID) community attributed to Kevin Ashton [1, 8], which focused on tracking the location and status of physical things to the more recently accepted description of converging the physical and digital worlds [1] where the network of many physical objects such as sensors, software, and network connectivity allow objects to exchange and collect specific data over the internet automatically or manually [9]. This continued growth of disruptive technologies leads the way for the next generation of IoT enabled ubiquitous sensing systems in smart homes. Examples include smart appliances, and systems including environment, utilities, entertainment and security control systems which compared to the more traditional methods of control mechanisms can be operated from anywhere utilising cloud technologies [10, 11].

As a rule of thumb, the proliferation of IoT sensors and devices requires modern security controls and data sharing models. Luckily, we have seen an evolution in related transformational technologies such as Blockchain. Blockchain can prove to be a method to ensure a much more joined-up and integrated approach to data sharing including when processing sensitive data such as clinical trials [12, 13]. We think this technology can be utilised to further support this type of collaborative systems.

2.2 Security Alarm System Approaches in Smart Homes

An Arduino-based home intruder alarm system [14] utilised laser light. The method consisted of a laser to detect movement and a buzzer to sound after motion has been

detected by the laser. The switch was used to activate and deactivate the laser and the Arduino microcontroller to make the system operate, function and work. The main concept of this idea involved the laser security system is fully activated by the switch which the resident had to activate. The laser would trigger if an object passed between the laser light and light-dependent resistor, causing the buzzer to go off and alarm the resident, indicating an intruder. According to [14] the test results from the prototype system achieving an overall 80% success in detecting intruders by tripping the laser.

The authors in [15] proposed a Rochelle salt integrated Passive Infra-red (PIR) sensor Arduino based intruder detection system. The method consisted of a PIR sensor for suspicious movement detection and a Rochelle salt used as another sensing element to reduce the false alarm rates. Additionally, an internal buzzer was implemented to alert the resident of an intruder after a motion was detected within the home. The main concept of this idea is that when an intruder trespassed into a home, the PIR sensor would detect movement, which caused the alarm to go off and sound, alerting the resident of a burglar. According to the authors [15], the Rochelle salt improved the system's performance, achieved a more efficient detection and decreased the false alarm rate.

Another study [16] proposed a unique IoT Arduino based door unlocking security system with real-time control for a home. The system consisted of an Arduino microcontroller, RFID reader and tag, wireless transmitter and receiver, a database and a webpage. The main concept of this idea involved improving the security of homes, offices, laboratories and libraries, by monitoring authorised individuals' movements in and out of a building thus preventing unauthorized individuals from gaining access. To gain entry, an authorised individual would have to swipe the card on an RFID reader in order for the system to authorise access. Once authorised, the information was transmitted wirelessly and stored in an online database. Access logs registered successful and denied access and the date stamp, which could be monitored by an authorised individual for a potential unauthorised entry. According to the authors [16], the door could be remotely controlled from anywhere in case of emergency. In addition, the authors asserted that their proposed security system is efficient, secure with a capability to remotely monitor the movement status including unauthorised entry attempts in addition to the exit of authorised individuals.

Likewise, [17] proposed a unique IoT home security system. The system consisted of two modules. Module one included a 4x4 matrix keypad, Arduino Uno microcontroller, potentiometer, Liquid Crystal Display (LCD), Sonoff SV, electromagnetic lock and a 12V (Volt) power bank. The second module consisted of Global System for Mobile Communications (GSM), Infrared Camera, PIR motion sensor, buzzer, battery backup. The main concept of this idea utilised the first module to control the door locking and unlocking with the electromagnetic lock. The LCD showed the status of whether the attempted door access was authorised or unauthorised after the password was entered by the individual wanting to gain access via keypad. If the password matched, then a signal was generated and sent to the Arduino microcontroller to allow the door to be unlocked. The second module was utilised and activated when the residents were away

from home. Once the second module was activated it worked in parallel with the first module. The security was enhanced by the PIR motion detector with the alarm sounding, infrared image capture and an SMS message sent to the owner via a GSM module alerting the owner of an intruder.
The comparison of the different approaches to home security systems outlined in this section is summarised in Table 1. Whilst the investigated Arduino-based home intrusion detection systems dealt with the problem of sounding an alarm to alert the residents, only one of the investigated studies presented a feature to alert the owner utilising a GSM module. The problems that continue to persist in protecting smart homes are the absence of convergence between the physical components, the digital domains and people, lack of real-time interactive risk-based monitoring and protection of vulnerable and marginalised groups. The solution to this problem is presented in the concept of an IoT community-cluster model for burglar intrusion detection and real-time reporting in smart homes.

Table 1. Comparison of different approaches to home intrusion security systems

Study	Does the proposed system alert the owner?	Does the proposed system have the capability to alert the police or an ARC?	Is the proposed system designed in a way to protect vulnerable and marginalised groups?
[14]	NO	NO	NO
[15]	NO	NO	NO
[16]	NO	NO	NO
[17]	YES	NO	NO
This Study	**YES**	**YES**	**YES**

3 System Design

We present the IoT Burglar Intrusion Detection (I-BID), the I-BID home security alarm system aims to converge the physical, digital and people realms, achieve real-time monitoring and alerting, and design a solution in a way that is inclusive of vulnerable and marginalised groups. How these aims are achieved is described in detail in the remainder of this section, by producing a design schematic, unique pseudocode and the related data flow diagrams. The key strength of our system is the novel design which enables the communication process in real-time to multiple recipients autonomously and simultaneously compared with proposed systems in other studies.

3.1 I-BID Schematic Design and the Dataflow

The main system components which are presented in Fig. 1, consist of the HC-S04 motion sensor, the WiFi shield and the Arduino Leonardo microcontroller board. The

WiFi shield is wired to the Arduino Leonardo microcontroller board to connect to the internet and communicate with online services to establish the wireless capabilities for the SMS, and it is wirelessly connected to a home router, which creates the capability to autonomously and simultaneously interact in real-time with multiple recipients. This could include the owner, community-based smart-neighbourhood-watch type buddy, ARC and including law enforcement. That said, although the presented concept creates this capability, the authors acknowledge that in the UK the police trigger is strictly regulated [7]. The data flow diagram highlighting the key system processes is shown in Fig. 2.

The connections were made to their appropriate inputs in approximately four steps to wire the system:

- The first step was to connect the Ground (GND) from the ultrasonic sensor t GND on the Arduino Leonardo microcontroller.
- The second step was to connect the Voltage Common Collector (VCC) to 5V on the Arduino Leonardo microcontroller.
- The third step was to connect the echo pin, which will be directly connected to pin 4.
- In the fourth and final step, the trig pin was connected directly to pin 2 on the Arduino Leonardo microcontroller, which allows ultrasonic waves to be sent out that allow motion to be detected.

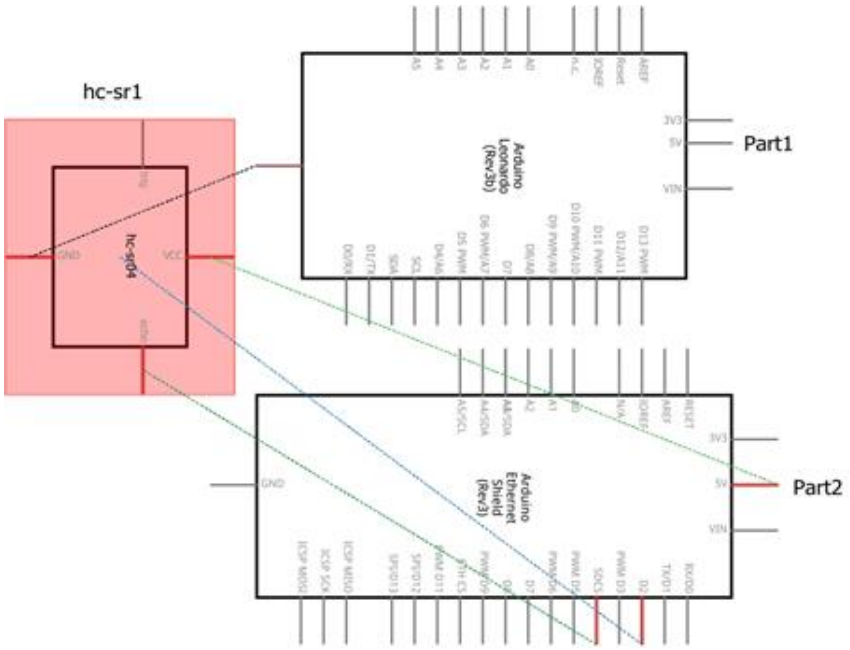

Fig. 1. Schematic Diagram of the I-BID home security alarm system.

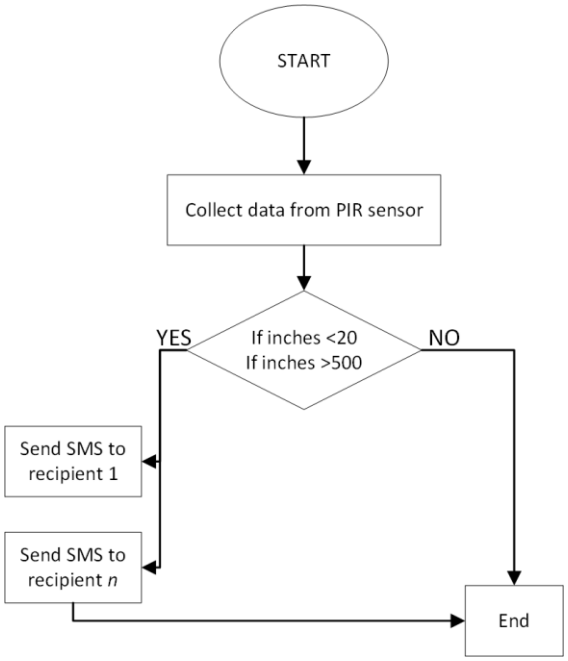

Fig. 2. Dataflow the I-BID home security alarm system.

3.2 Pseudocode

The pseudocode for the I-BID home security alarm system is outlined in **Error! Reference source not found.**. The ultrasonic sensor sends the SMS message via WiFi, in this case, the WiFi shield. The sensor communicates with a service called Temboo which utilises a Twilio account where the numbers are set for the SMS recipients, which then sends a chore SMS to the selected recipients' phone numbers.

Table 2. The Pseudocode for the I-BID home security alarm system.

Start
1. Activate system
2. Ultrasonic Sensor will calculate distance from the sensor to the closest object in front automatically
3. After Ultrasonic Sensor has measured its distance, then println "system ready"

```
LOOP
    4. IF inches are less than 20 or/II if it is greater than 500 / motion is detected
    5. Println “Intruder detected, sending the SMS notification”
    6. Communicate or call the Temboo client
    7. Set the Temboo account credentials/app key name
    8. Set choreo inputs/set phone numbers of who the SMS will be getting sent to
    9. Send SMSChoreo to interlinked phone numbers.
While
    10. While SMS is sending
    11. Tell the process to run and wait for results to see whether or not the SMS has been sent?
IF
    12. If return code is 0,
    13. Serial. Println “SMS SUCCESSFULLY SENT”
    14. Success = True
} Else {
    15. If no return code of 0, then SMS has not been sent.
    16. Serial, println “SMS has not been sent”
     }
 }
    17.  SendSMSchoreo.close
    18. Delay for 10 seconds
    }// end if statement
}//End loop
```

The following steps are described by the pseudocode:

- Step 1: initially activates the system.
- Step 2: the ultrasonic sensor calculates the distance from the sensor to the closest object in front to get ready for detection.
- Step 3: prints a comment that indicates when the sensor has finished measuring the distance and is ready to detect.
- Steps 4-9 is processed within a loop:

  - Step 4: If the distance deviates from the sensor measurement completed in step 2, then motion has been detected.
  - Step 5: prints “Intruder detected”, sending SMS alert after motion is detected.
  - Step 6: calls the Temboo service which allows access to the Twilio account so that a choreo SMS message is sent to the selected recipients simultaneously.
  - Step 7 and 8: to successfully send the SMS, phone numbers and an app key name have to be added to the algorithm. More specifically, these numbers are the numbers that are set up on the Twilio service.
  - Step 9: after Temboo and Twilio have communicated with each other, the SMS message is sent via the carrier network to the selected and added phone numbers after motion is detected by the sensor.
- Steps 10 and 11: is where, while SMS is sending to the pre-set phone numbers, instruct the process to give feedback on results to find out if SMS was successfully sent.
- Steps 12,13,14: consist of telling the process, if SMS has been sent, then return 0, with
- Steps 15 and 16: involving else if 0 has not been returned, then prints “SMS has not been sent”.
- Steps 17 and 18: by ending the process of sending the SMS, ends the overall process.

4 Constructing and testing the I-BID home security alarm artefact

During the construction phase, component-level testing was carried systematically to analyse that components within the system, Fig. 3 are operating and functioning according to the design criteria. This was achieved by using a test-table method while constructing, Table 3. The table consisted of six columns: “Test ID”, ”Test Reason”, “Expected outcome”, “Actual outcome”, “Pass/Fail”, “What will be investigated to fix the problem, and how was the problem fixed”.

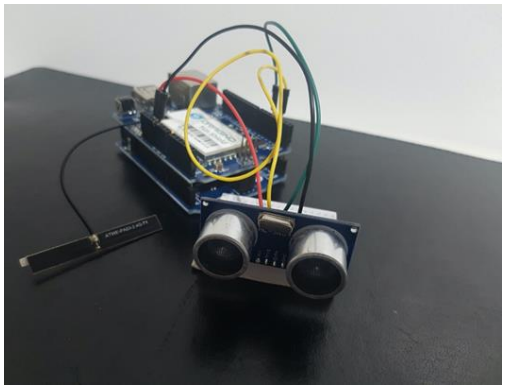

Fig. 3. The sensor has been connected to the WiFi shield.

Table 3. Functionality testing of the I-BID home security alarm system

Test ID	Test Reason	Expected outcome	Actual outcome	Pass/ Fail	What will be investigated to fix the problem, and how was the problem fixed
TEST TABLE 1					
ID 1	To test if the WiFi shield is successfully connected to the personal router.	Connected	Connected	PASS	N/A
ID 2	To test signal strength for connection strength and reliability between WiFi shield and personal router	Signal strength between 50-60%	62-68%	PASS	N/A
TEST TABLE 2					
ID 3 (First test run for sensor)	Test the sensor to see if the distance is measured/detects correctly between the sensor and the wall, and motion in-between	Distance to be measured continuously and only stop as soon as hand/motion is placed in front of the sensor with an output saying "intruder has been detected!!!!" in the serial monitor	A repeated message in serial monitor saying "intruder has been detected!!!!" without anything being placed in front of the sensor	FAIL	**Investigation** - Bugs in code - Wrong wiring connections - The incorrect distance set within the code - Faulty hardware/sensor
ID 3.1 (second test run for sensor)	Test the sensor to see if the distance is measured /detects correctly between the sensor and the wall, and motion in-between	Distance to be measured continuously and only stop as soon as hand/motion is placed in front of the sensor with an output saying "intruder has been detected!!!!" in the serial monitor	Distance measuring correctly and says "intruder has been detected!!!!" within serial monitor when hand/motion is placed in front of the sensor	PASS	**Problem found:** - Set Distance was incorrect within sketch /code **How the problem was fixed:** - Distance changed to correct distance
TEST TABLE 3					

ID 4	Testing if SMS is sent to both recipients after the ultrasonic sensor detects motion.	SMS sent to: *Recipient 1* "Intruder has been Detected!!!!" *Recipient n* "Intruder has been Detected!!!!"	SMS received by: *Recipient 1* – "Intruder has been Detected!!!!" *Recipient n* - "Intruder has been Detected!!!!!	PASS	N/A

The code is shown in Fig. 4. outlines the steps of when the sensor detects movement, the sensor communicates with Temboo service, which communicates with Twilio and tells Twilio to use the specified phone numbers to send an SMS to the selected phone numbers alerting them of intrusion. Twilio details, specifically the number that will be used to send an SMS message to the recipients, has been activated and implemented within the code, Fig. 4, and uploaded to the Arduino Leonardo microcontroller board.

Fig. 4. The recipients' phone numbers added to the code. Note: some personally identifiable information has been hidden.

The test shown in Fig. 5 visualises tests 3 and 3.1, Table 3. In this test, we examine if the distance is measured correctly between the sensor and the wall, and the motion is detected in-between. This was achieved by placing an object, hand in this case, in front of the sensor, to test if the sensor triggers the code and the SMS is sent to the recipients' phones alerting the recipients of the detected intrusion in real-time.

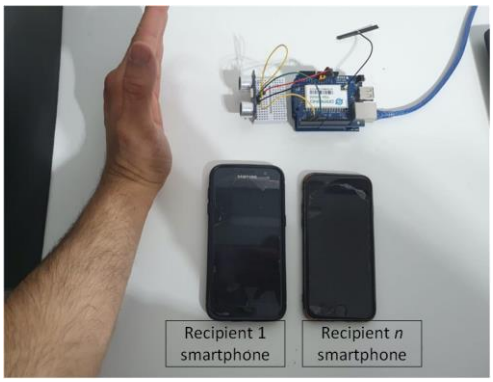

Fig. 5. Placing a hand in front of the sensor to investigate if motion has been detected and SMS has been sent to the recipients.

The test shown in Fig. 6 visualises test 4, Table 3. In this test, we examine that test of sending and receiving the SMS was positive, and expected results were achieved. After the object, hand, in this case, is placed in front of the ultrasonic sensor, An SMS text message was successfully received with the expected body of the message "Intruder has been Detected!!!!". Both messages were received simultaneously and autonomously at the same time, which also achieves a key aim of this project.

Fig. 6. SMS Intruder alert sent to the recipients' mobile phones successfully in real-time on the left-hand side of the figure and a clearer view of SMS sent on the right-hand side of the figure.

5 Evaluation of the prototype artefact

The prototype artefact's performance was validated against the design criteria. Two smartphones shown in Fig. 7 below are placed within the system to visualise the recipients' phones ready to receive an SMS alert after motion is detected by the sensor.

Fig. 7. Prototype artefact I-BID home security alarm

As soon as the home entry point was breached, the door, in this case, the sensor above the door has detected motion and sounded off the alarm, and the sensor that is connected to the WiFi shield facing directly towards the door has also detected that motion, and successfully sent an SMS utilising the WiFi directly to the designated recipients' mobile phones autonomously and simultaneously in real-time, Fig. 8.

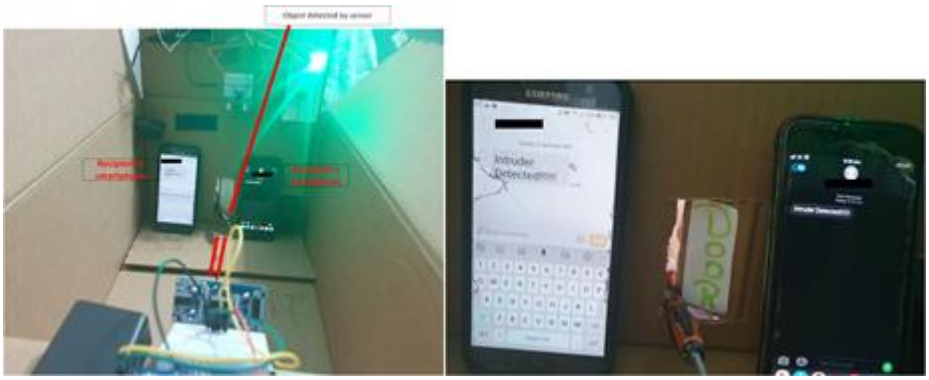

Fig. 8. SMS Intruder alert received by the designated recipients on both smartphones autonomously and simultaneously in real-time on the left-hand side of the figure and a clearer view of SMS received on the right-hand side of the figure.

We produced enhancements to the home security alarm systems compared to the methods of previous studies, Table 1. The improvement was achieved by converging the physical components with a unique algorithm and leveraging IoT to alert residents in real-time when an intrusion in their home is detected. The new capabilities around

alerting multiple recipients autonomously and simultaneously in real-time have been tested and validated empirically iterating through the design phases and the final artefact. More on the collaborative approach of I-BID will be discussed in the next section.

6 How can the I-BID home security alarm improve homes security collaboratively

Traditional home security alarm systems secure homes individually relying on human intervention. However, this is no longer sufficient, and we argue that IoT-based real-time security mechanisms are required as a forward-looking approach. This assertion is supported by the following survey [18] in which Citizen Advice aimed to gain an understanding of consumer protection expectations of what the consumers would expect to be a norm within smart homes. The participants responded that manufacturers of smart locks should identify unusual behaviour proactively and alert the consumer as a burglary preventative measure.

We illustrate parallels with the field of cybersecurity. According to [3, 19] authors assert that despite digitalisation and transition from traditional to an IoT enabled practice, there appeared little evidence of cross-organisational information security sharing and coordination across smart city sectors. Furthermore, practices appeared in silos and lacked cyber-defence collaboration [19]. We argue that a similar phenomenon can be found in smart homes security. Despite the transition from traditional to smart homes leveraging IoT, home security operates in a silo approach. An example being the alerting process which is maintained in a tightly controlled central management structure with a human in the loop. Therefore, advanced and forward-looking solutions are required to support a modern and collaborative home defence approach.

The empirical evaluation of the artefact formed a critical part of demonstrating that the I-BID home security alarm system can be scaled as a community cluster model. Our approach is inspired by the concept of a community-led neighbourhood watch scheme [20], which is potentially a critical factor for vulnerable and marginalised groups.

7 The I-BID Community-Cluster Model for Burglar Intrusion Detection

Because the I-BID system can, by design, communicate with multiple recipients via appropriate communication channels, it can collaborate with homes within the neighbourhood such as chosen friends and relatives. This could be achieved by extending the artefact to utilise two sensors implemented within the same locations of different homes, as we outline in the I-BID community-cluster model Fig. 9.

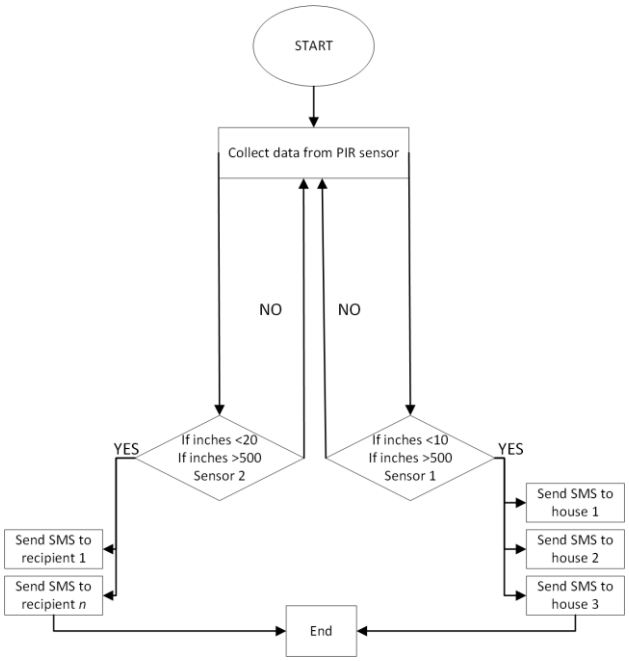

Fig. 9. I-BID community-cluster model for collaborative home security alarm system

Sensor 1 is placed at the home entry point such as outside of the front door. This sensor detects motion at the front door causing the system to collaborate with another system that is part of the community-cluster model within another home. That sensor alerts the resident and the neighbours in the cluster that a motion has been detected by the front door sensor of the collaborating house across the street to indicate that the partnered house is at possible risk of intrusion. This is considered low risk.

Sensor 2 is placed inside the home which will be facing towards the home entry point such as the front door, ready to detect motion and send an SMS alert autonomously and simultaneously to multiple recipients in real-time to their smartphones alerting them of an intrusion. However, if an SMS is then also triggered from inside that home, it indicates that an intrusion is likely to have occurred. Therefore, the SMS is sent directly to the owner and the model has the capability to send an alert to an ARC or law enforcement alerting all specified recipients of an actual intrusion. That said, we acknowledge that whilst we have designed and demonstrated capability further research, development and empirical testing of the artefact is required.

The homes within the I-BID community-cluster model are federated at the Temboo service layer. To maintain privacy, each home is set up with its own I-BID system consisting of internal and external sensors, a minimum of a pair of sensors, Sensor 1 and Sensor 2. Sensor 1 is placed inside the home entry point and Sensor 2 is placed outside the home entry point. However, the model could support multiple pairs of sensors to be

placed at other home entry points e.g. back doors, side doors or windows. The WiFi shield utilises the local wireless router to enable secure communication with the Temboo service which is the layer where the homes are federated into clusters.

For example, in a small cluster of three houses, if Sensor 1 detects motion within home one, then the system will send an SMS message to alert the other two homes in the cluster of a potential intrusion. The same applies to the other two homes, hence, if Sensor 1 detects motion within home three, then home two and one will be alerted by an SMS text message. It is worth mentioning again, that if Sensor 2 detects motion that indicates high risk, then the system will directly send the SMS message alert to the owner and can communicate with multiple specified recipients. Therefore, this could include ARC and law enforcement contacts.

7.1 Cybersecurity implications of leveraging IoT in physical protection of homes

IoT based physical security of homes is an evolving field and whilst technologies and innovations that support the delivery of the objectives for homes' physical security are transformational, they also have numerous challenges. Apart from the multifaceted nature of issues such as privacy, ethical challenges and regulatory aspects, one of the key concerns of the IoT based physical protection of homes is cybersecurity.
Consumers desire to use cutting edge technology, comes with various challenges including the proliferation of smart technologies and the lack of understanding of associated risks and vulnerabilities [18]. Due to the threats such as data breaches or data interception, technical security mechanisms including authentication, access control, network and cryptographic protections are needed to protect information when shared systems intercommunicate wirelessly and when cloud services are utilised.

Furthermore, privacy and security need to be maintained between each collaborative home when information is shared to protect the confidentiality and integrity of the data. End-to-end encryption has a role to play as part of the layered defence in-depth approach, for example [21] discusses how the use of end-to-end encryption allows only the communicating users to open and read specific messages and research by [22] suggests that end-to-end encryption decreases the risk of attacks including a man-in-the-middle compromise.

7.2 Risk assessment

A risk assessment matrix for the sensor thresholds is produced for the collaborative approach, Fig 10. Sensor 1, being the sensor on the outside of the home entry point, if triggered, is considered unlikely that an intrusion has occurred, Fig. 11. Sensor 2, being the sensor on the inside of the home entry point, if triggered, is considered likely that an intrusion has occurred and the impact of such incident is considered high, which potentially according to Fig 10 could result in harm to residents.

Impact	Probability of the likelihood and impact	Likelihood				
		Very Unlikely	Unlikely	Possible	Likely	Very Likely
	No Impact					
	Low Impact		Sensor 1- outside the home entry point			
	Medium Impact					
	High Impact				Sensor 2 - inside the home entry point	
	Catastrophic Impact					

Legend – Risk Categories		
LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT

Fig 10. A Risk Assessment matrix for the I-BID community-cluster model

Sensors	What threat could occur	Who will the system alert	Risk rating priority /taking Action
Sensor 1 outside the home entry point	Attempted break-in	collaborated houses in the cluster	LOW
Sensor 2 outside the home entry point	Harm to residents/Aggravated burglary	Capability to alert multiple recipients including ARC	HIGH

Fig. 11. A Risk Impact matrix for the I-BID community-cluster model

8 Ethical considerations of burglar intrusion detection

At an individual level, the desire to use a security mechanism to protect the physical security of homes from potential intruders may give rise to questions of social injustice and equality issues such as affordability and accessibility of technologies and access to effective law enforcement response thus counterbalancing the desired effect of physical home protection as a deterrent of burglary related crimes. According to [23], the police-recorded crime data for England and Wales supports the notion of inequalities and crime including burglary. Furthermore, the author in the same study outlines a link between wealth and security mechanism adoption. Therefore, a commitment to developing a consistent and affordable approach to effective physical home security is required.

At a societal level, according to research by the Institute for the Study of Civil Society [24], a comparison of households with income of above £50,000 and below £10,000 showed that the low-income households were twice as likely to be burgled. Furthermore, this study showed that the households below the £10,000 income threshold were two and a half to three times as likely to live in fear of crime including burglary with further evidence of three and a half times the rate of criminals living in the 20% most deprived areas compared with the same rate in the least deprived areas. The link between wealth and security measure adoption and the level of insurance premiums of the

low-income households has been outlined by [23]. Questions could arise if wealth is the ultimate driver of home protection thus mechanisms would be required to make physical home protection available to disadvantaged groups.

9 Conclusion

Can physical security controls of homes be improved in today's era? This study aimed to improve physical security controls within homes regards burglar alarm systems, which could help burglary and intrusion decrease in this day and age. Office for National Statistics [4] stated that there has been an increase of robberies by 12% in 2019 compared to the previous year, and still increasing to this day. Part of this problem was because of weak physical security controls implemented within homes. However, physical security controls that are implemented within homes are not always fit-for-purpose; they fail to alert residents in time of unauthorised access, slow response by police, and false positives. These issues signals why robberies are not decreasing, which is a big current issue that needed to be dealt with and solved. Therefore, our objective was to propose a new and improved IoT based home security alarm system that could offer better protection for homeowners including vulnerable groups of people (e.g. disabled people) from burglary. Nonetheless, reasons for unauthorised access are not always linked to burglary, as it could also include hate crimes and domestic abuse [25], hence the need for a collaborative approach with community support facilitated by technology. The empirical evaluation of the proposed design in this study has formed a critical part of demonstrating that the I-BID home security alarm system can be scaled as a community cluster model. Our approach is inspired by the concept of community-led neighbourhood watch schemes, which is potentially a critical factor for vulnerable and marginalised groups.

References

[1] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and internet of things," 2019. 10.6028/NIST.SP.1900-202

[2] G. Ahmadi-Assalemi, H. M. Al-Khateeb, C. Maple, G. Epiphaniou, Z. A. Alhaboby, S. Alkaabi, and D. Alhaboby, "Digital Twins for Precision Healthcare," *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, pp. 133. 10.1007/978-3-030-35746-7_8

[3] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review," *Smart Cities*, vol. 3, no. 3, pp. 894-927, 2020. 10.3390/smartcities3030046

[4] Office for National Statistics, "Crime in England and Wales: year ending June 2019," pp. 66, 2020.

[5] Office for National Statistics, "Crime in England and Wales: year ending September 2020," 2021.

[6] Office for National Statistics, "Nature of crime: burglary dataset," ONS, ed., 2020.

[7] National Police Cheifs' Council, "National Police Cheifs' Council Security Systems Policy," https://www.policesecuritysystems.com/national-police-chiefs-council-security-systems-policy, [09/05/2021.

[8] K. Ashton, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97-114, 2009.

[9] K. K. Patel, and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," 2016. 10.17148/IARJSET.2018.517

[10] M. Asadullah, and A. Raza, "An overview of home automation systems." pp. 27-31. 10.1109/ICRAI.2016.7791223

[11] A. Modarresi, and J. P. G. Sterbenz, "Towards a Model and Graph Representation for Smart Homes in the IoT." pp. 1-5. 10.1109/ISC2.2018.8656928

[12] H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, *Blockchain and Clinical Trial: Securing Patient Data*: Springer, 2019.

[13] N. Ersotelos, M. Bottarelli, H. Al-Khateeb, G. Epiphaniou, Z. Alhaboby, P. Pillai, and A. Aggoun, "Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study," *Journal of Sensor and Actuator Networks*, vol. 10, no. 1, pp. 1, 2021.

[14] A. B. Arjona, P. K. M. Bautista, J. E. Edma, M. I. J. P. Martel, E. D. N. Octavio, and N. P. Balba, "Design and Implementation of an Arduino-Based Security System Using Laser Light."

[15] S. S. Saini, H. Bhatia, V. Singh, and E. Sidhu, "Rochelle salt integrated PIR sensor arduino based intruder detection system (ABIDS)." pp. 1-5. 10.1109/ICCCCM.2016.7918228

[16] S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, "Arduino based door unlocking system with real time control." pp. 358-362. 10.1109/IC3I.2016.7917989

[17] R. Kumar, and P. Mittal, "A Novel Design and Implementation of Smart Home Security System: Future Perspective," *International Journal of Applied Engineering Research*, vol. 14, no. 2, pp. 363-368, 2019.

[18] Traverse, "The future of the smart home: Current Consumer attitudes towards Smart Home technology," https://www.citizensadvice.org.uk/Global/CitizensAdvice/Energy/Smart%20homes%20final%20report%20(new%20Traverse%20logo).pdf, [13/05/2021, 2018].

[19] G. Ahmadi-Assalemi, H. M. Al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani, and P. Pillai, "Federated Blockchain-Based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace." pp. 1-9. 10.1109/ICGS3.2019.8688297

[20] N. W. Network, "Neighbourhood Watch National Crime Community Survey 2020," https://www.ourwatch.org.uk/sites/default/files/documents/2021-01/Neighbourhood%20Watch%20National%20Crime%20and%20Community%20Report%202020.pdf, [13/05/2021, 2020].

[21] M. Nabeel, "The Many Faces of End-to-End Encryption and Their Security Analysis." pp. 252-259. 10.1109/IEEE.EDGE.2017.47

[22] M. Thomas, and V. Panchami, "An encryption protocol for end-to-end secure transmission of SMS." pp. 1-6. 10.1109/ICCPCT.2015.7159471

[23] T. Newburn, “Social disadvantage: Crime and punishment,” *Social advantage and disadvantage,* pp. 322-40, 2016.

[24] P. Cuthbertson, “Poverty and Crime: Why a new war on criminals would help the most poor,” 2018.

[25] Z. A. Alhaboby, H. M. Al-Khateeb, J. Barnes, H. Jahankhani, M. Pitchford, L. Conradie, and E. Short, "Cyber-Disability Hate Cases in the UK: The Documentation by the Police and Potential Barriers to Reporting," *Cybersecurity, Privacy and Freedom Protection in the Connected World.* pp. 123-133.