Ensuring Effective Secure Learning Environment using Authentication System in Terms of Cost and Time at Kumasi Technical University, Ghana.

Abstract

A welcoming environment is important to promote learning activities in a tertiary institution. Students' violence has become a major concern in developing countries like Ghana. There is therefore the need to provide a system that will offer assistance to ensure or minimize this violence from students in other to provide tranquil learning environment. With the use of technology like Radio-frequency identification (RFID) the security of Kumasi Technical University (KsTU) can be up graded. Considering the enrollment of staff and the number of students, physical checks for security will demand time and cost. In this paper, a system which does not consume time, very efficient and cost effective will be utilized to oversee the physical security of KsTU. RFID and Local temporary capacity administration can also be used to manage student's attendance database server.

Two algorithms will be presented for efficient communication between the database server and nearby gadgets which will be raspberry pi. A discussion will be done to assess the time and cost involved in student verification authentication process and attendance. This paper is a theoretical analysis of the proposed system.

Keywords: **Raspberry Pi, Radio-Frequency Identification, Kumasi Technical University, Security, Authentication, Cost, Time, Algorithm, Environment.**

1. Introduction

It has become critical for Kumasi Technical University to provide strong security not just because of its valuable interior asset, but also to protect its teaching staff, administration, and students as well as guest. Whereas equipped

security guards add human component to the layer of security, a high-performance security system can also offer assistance in screening and checking human access to the university campus [1]. The security of students, faculty and administrators is important because of violence generating from misunderstanding, and demonstration just to mention a few. It may be difficult and a challenging task to provide a secure, solid learning environment. Due to this it has become a necessity to confirm all those who enters the premises of the university campus. Upon entry to the campus the student or staff/faculty credentials given are compared with that of the records of authorized individuals stored in the remote database Management system of the University.

Authentication here means that an individual identifies his identity by sending an input to a system, the system then confirms the input by computing and further checks that it equals the information in the university database [2].

The paramount responsibility is to ensure that a suitable security authentication measure strategy is required to protect the assets of Kumasi Technical University. Multi-factor authentication is ensured for effective authentication. These are knowledge, possession, and inheritance [3]. The authentication process is popular said to be something you know, something you have and something you are, respectively [3, 4]. Knowledge factors: demands the user to illustrate Knowledge of hidden information. This may come in form of passwords, pins, and answers to a secret question and so on [5]. Possession factors are physical entities had by the user to client computer or university portal. Example: security token, locker key RFID tag etc. Inherence factors come with a measure that naturally are claimed by the authorized user. These regularly takes the form of biometrics such as unique figure prints, voice recognition, eyes etc. These factors are designed to guarantee that unapproved users cannot pass through the authentication process because they are almost 100% unique processed by the authorized user [6]. The system also stores the time the user was authenticated. Here the process for authentication can be grouped into two categories: physical authentication and the use of technology to authenticate individuals who enter the university campus.

2. Literature Review

2.1 Utilizing Physical Security

Safeguarding important and confidential information, networks, software, infrastructure, institutional assets, and personnel's calls for the need of physical security. If physical security is not managed properly, all strategies put in place will be useless once an attacker gets through by gaining physical access to the university campus [7].

Physical security can serve as a measure to give access to only authorized individuals or users. (Only after authentication). Physical security comes with its own disadvantages, as it is human driven. Examples placing security guards at the gate/ main entrance may need a licensed gun/guard house, training, uniform and what have you. These measure in turn comes with cost and it is time involving (there is always a need for a security guard to be at the entrances) [8].

Aside the above-mentioned problem, employing security guards will not be enough because the guard may not be able to monitor all activities of the crowd and may also allow unauthorized people in through personal relationship and by accepting bribery [9].

As mentioned before, measure used for physical security such as fence, wired-fence, security guards, are few and no one pay head heed to the attention on physical security as it on technology-oriented security. To overcome the problems associated with utilizing physical security an alternative mechanism for authentication may be considered.

2.2 Utilizing Technology for authentication

The most important improvement you can make to authenticate security is by adding technology utilization to it. In that way even if an authorized person get through there will be confinements to move advance which can in turn make obstruction to passage. Considering the number of students, faculty and administrative staff, that needs frequent authenticating employment, physical security will be costly and involving [10]. The use of technologies such as password, smart cards digital certificate, Kerberos, barcode system and RFID, do have their draw backs, based on the strength of the technology selection that can be made. For better appreciation of the various authentication system, an exhaustive outline of their conventional and modern use is considered. Where the technology will be, how it will be used, and when it will be used must be weighed before the technology will be implemented. The pros and cons of the authentication technology must also be considered. The distortion of voice due to sickness and at times age factor is another drawback for voice recognition systems, and so will a fingerprint system may not be able to recognize a fingerprint due to a damaged finger making it difficult for the system to

recognize it. This technology may have its draw backs. For example, passwords can easily be changed at times when the user feels in secured but with face authentication methods, things are totally different. One cannot alter an already designed security set up of system device unless the user gets physical access to it [11]. Therefore, in case a thief get access to your phone the thief may be motivated to use a fake silicon finger, to trick the fingerprint reader unlock the phone and retrieve all interest information stored on the memory of the phone [12].

One disadvantage with biometric authentication is that if an information gets hack it become difficult to recover because users can't change their facial recognition easily as it is with passwords.

2.3 Attendance using Authentication security system

Attendance plays a vital role in students' academic performance. The learning of a subject is significantly influenced by participation of the lectures through attendance and workshops of that subject. [13]. In most academic institutions, the attendance may be a manual register entry and human driven verification approach, which can cause issues of incorrectness, losing registers and longer time consuming. Lectures may additionally show bias in the participation responsible of a student just like the security guard might do in the event of utilizing a physical security. On the other hand, we might utilize, RFID technology to develop an attendance system that would decrease the time involved in checking attendance and the deceitful passage in the participation registers may also avoid human mistakes. The system has UIs panel for student, faculty, and administrations. Students will actually want to see their attendance and create report through the students' panel. Lecturers' panel will empower them to see student attendants and also creates report. The administration panel will allow the administrator to have all the privileges of the system to perform their task.

2.4 Security System in Educational Institution

Addressing the security issues of a tertiary educational institution, it is vital to concentrate on the satisfactory risk levels which are setup by the government of Ghana and the technical university policies. These risks should be

considered as the maximum passable beneath the genuine conditions of the financial, technical, and social state of the country.

For the coordinate execution of the standards of government laws against fear of terrorism, assuming the safety of the population and domain from crisis circumstances of normal and man-made disasters, fire security must be considered as one of the specifics of the educational institution. This makes it critical to protect the institution from its generations of intruders. Thus, boosting the institution's confidence in their day-to-day learning activities without the fear of violent activities. By doing so, the institution can improve attendance, reduce anxiety, and support behavioral regulations of students and their faculty. The security of students, faculty, administrators, and other valuable assets are of very high importance to the institution.

To ensure utmost security of the educational institution, time, cost, and the type of security needed must be well considered. This is because, both students and faculty may need to enter campus for lectures at the same time, and either before or after the start of lectures. In implementing a security system to check and verify individual identity, the system should be effective and efficient one in terms of its cost and time consumption.

The objective of this paper is to develop RFID Basic Access Control System for physical security and automate system for attendance at Kumasi Technical University.

2.5 History of RFID Technology

Exploratory science started in the Nineteenth century. Michael Faraday in 1846 suggested that light and radio waves are the piece of electromagnetic range. In 1864, James Clerk determined that electric and magnetic field travel at speed of light in transverse wave form. Rudolf Hertz was the primary individual who send and got radio waves in 1887. Guglielmo Marconi in 1896 led the effective

Trial of transmitting telegraph across Atlantic followed by Ernst F.W Alexanderson producing and sending continues radio waves in 1906 [14]. Radar was created in 1992 followed by improvement of IFF (If companion or enemy) framework in 1937 and 1938. In 1940s numerous refinements in these frameworks was completed and RFID was imagined in 1948 after the distributing of Communication by mean of reflected force by Harry Stockman [15, 16]. From 1950s to 1960s, inventers and organizations were occupied in investigating the RFID innovation to foster RFID based gadgets. That time was additionally the start of the business use of the RFID. Electronic Article observation (EAS) gear was created to counter burglary. Detached labels were created in 1975. RFID framework

was taken advantage of for electronic cost framework and the world first cost framework was opened in Oklahoma in 1991. RFID frameworks installed to the organizations to use the production network furthermore, Assembly line. In 2008, drugs maker utilized it for the shipment of the genuine items to the drug stores to help them recognize fake or implied one. Clinical gear producer utilized 60% RFID in their items, and it was too utilized in electronic records simple for ID purposes. RFID is winning from scholastic organization to corporate organizations [14]. Examples of applications that uses RFID are access control for people, vehicles, manufacturing automation, logistics, product security, maintenance, and other numerous application areas.

Characteristics	Finger printing	Voice Recognition	Face Recognition	Iris Recognition	RFID	Barcode	Manual
Cost	Medium	High	High	High	Medium	Medium	High
Accuracy	High	Low	Low	High	High	High	High
User Training	Medium	High	Low	High	Low	Medium	Low
Technology	Biometric	Biometric	Biometric	Biometric	Wireless	Optical	Human
Physical Contact	Yes	No	NO	NO	NO	Yes	NO
Time Consumption	High	Medium	High	High	Low	High	High
Environmental Effect	Medium	High	High	Low	Medium	High	Low
Security Severity	High	Medium	High	High	Low	Low	Low
User Age Effect	No	Yes	Yes	NO	NO	NO	Yes

Table 1 Comparison of Characteristics of Different Authentication Systems.

3. Materials and Methods

3.1 Proposed System Architecture

To improve comprehension of the authenticating system, the general authenticating system worked using three levels or levels design as displayed in Figure 1.

The first level interface with the external environment, these involves the use of RFID and web base end UIs for example Student panel, instructor panel and administrator panel. The subsequent level is middleware connecting the database server to RFID and UIs. The third level is the backend of the authenticating system. This contains the database server connecting to the RFID and user interfaces for storing and recovering of data. The architecture of the authenticating system would use Local Area Network (LAN). Transport Control Protocol/Internet Protocol (TCP/IP) is utilized to establish connection between the database server and middleware before communication. Web based user panels are facilitated on Local web server and Hyper Text Transfer Protocol (HTTP) is for correspondence between client PCs and web server utilizing LAN router(s). All other gadgets would be utilizing the same network, static IP addresses are allocated to the database server and middle layer (including web server) to avoid longer time utilization by Network address interpretation (NAT). So the IP located to the database server and the middleware never change after setting up the authenticating system. Dynamic Host Configuration Protocol (DHCP) is designed on these routers to allocate dynamic IP locations to the client PCs. IP address returns once again to the IP address Pool of DHCP when the client is off. Considering the height and movement of young people, at the main gate an RFID reader will be placed at one side of it with the motion sensor placed two feet away from it horizontally and 7 feet from the ground there will be another motion sensor placed vertically.

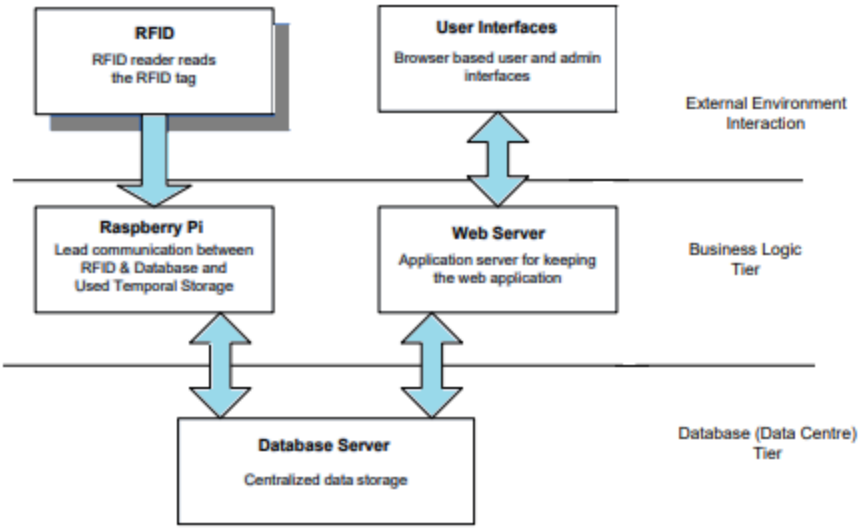

Fig 1: The Proposed System as a Three Tier Architecture.

At the hour of authenticating system commencement, the entire identification numbers or RFID tags are sent to the middleware at main gate for actual security validation of people. The individual needs to pass through the motion sensor and afterward RFID reader at the entryway of the main gate. The RFID reader at entryway read the identification number from the student or staff card when somebody passes through it. At this point, when the movement is recognized by sensor, then, at that point the individual is allowed through the entryway in the event that they have distinguished proof number (RFID tag) on student or worker card. The identification number is then exchange to the middleware for query purposes. False outcome will be produced by turning on the red LED (Light Emitting Diode) for the portrayal of the unapproved individual (an individual has no identification number or then again has invalid identification number and entered through the entryway).

At the point when an individual passes through the motion sensor, by three seconds the authenticating system read the identification number of that individual through RFID reader. At the beginning, every lecturer's, identification numbers or RFID tag of students are queried from the database server to the middleware. The authenticating system needs to check whether a student has a class at the selected classroom and subject by checking ID number from tag installed in the student card through RFID reader and contrasting it against the queried records in the middleware. Green LED is turn on in case result is valid and the student needs to go through the motion sensor to record the

participation. The identification number (participation record) is stored locally by Raspberry Pi middleware after the location of movement by the sensor. When the predetermined span for authorization to enter the class is done, the participation status of the relative multitude of records are sent back to the database server for permanent storage.

The UIs are facilitated on the nearby web server, when somebody connects with the nearby LAN and request to the web server for their respected panels trough web browser, the web server handles the request and UIs are stacked to the user PCs. Admins UI issued to add, delete, update, and view student record, faculty members record, timetable, student participation, and subject. Faculty members can queried for student attendance through the UI intended for them. Comparative, student can view their class attendance using the respected UIs. The IP addresses are dynamically assigned by DHCP configured router to the user PCs to connect it to web server.

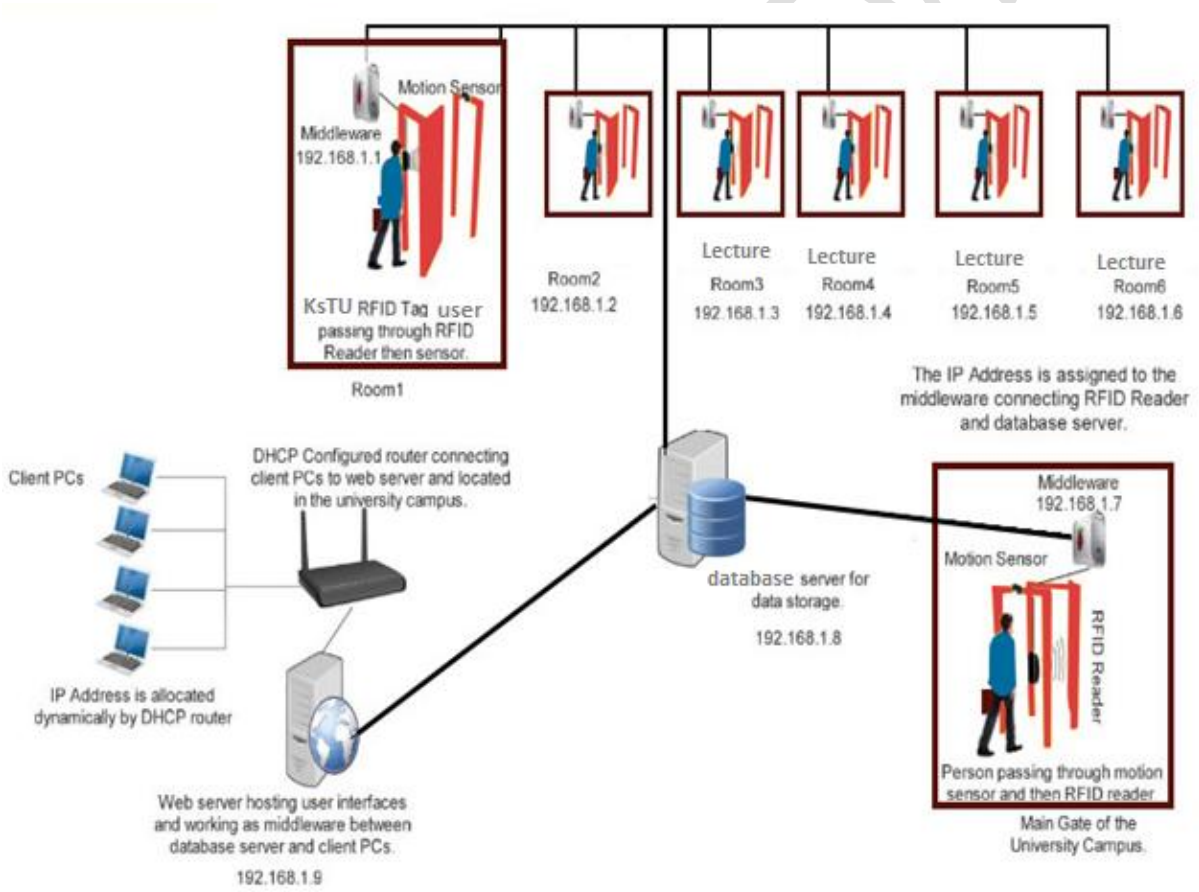

Fig. 2. The Proposed System Infrastructure and its Working Mechanism

How Efficiency Is Accomplished?

3.2 Efficiency of the Proposed Authenticating System

The proficiency as far as time is concern for the authentication System is achieve by two methods,

Method 1; at the main gate and Method 2; at the lecture room to verify attendance.

Kumasi Technical University has over 11000 students and over 700 staff (both academic and administrative staff), authenticating such numbers needs a flexible system in terms of time. At busy times such as school re-openings the entries are excessively enormous, which needs a productive system to verify all the entries without any deferral and without system disappointment. Normally, class address time is 60 minutes, including attendance time for roughly forty students, which is a tedious and time demanding process. Essentially Kumasi Technical University has various divisions in terms of; lecture rooms, students, faculty members, administrators, and complex timetable to deal with proficiently.

So, we have accomplished the general proficiency of the proposed system by using the innate proficiency of the RFID technology and interfacing the database server with RFID in an efficient way to prove proficiency.

3.3 RFID Proficiency

RFID utilizes radio waves and are quicker than other technologies like biometric and standardized identification reader like barcode, as there is no need of the actual contact between the RFID reader and RFID tag. Tag is the chip in the students or staff card on which the ID number is saved. The information is moved to the reader from the tag and when the tag is brought to the electromagnetic field of the reader minus any additional preparing information that may cause noise and pressure as needed in biometric and scanner tag framework [15]. The RFID reader then exchanges the information to the middleware (Raspberry Pi machine) situated close to the RFID reader which contains every one of the brought records and associates RFID reader to the database server.

3.4 Control Productivity

The database server and RFID reader are interfaced through Raspberry Pi functioning as middleware. This middleware communicates with both database server and RFID reader. At the main gate all students and staff

records are gotten once to the raspberry pi, to save from regular correspondence (frequent requests for authentication at each entry) to the database server.

Despite of verification of each record at the server is replaced by local repository check in the raspberry pi.One more approach to improved proficiency is to be doled-out static IP locations to the database server and middleware's (including web server) at the hour of system arrangement to save it from time utilization by Network address interpretation (NAT), as all these gadgets are consistently on the same Network. Likewise, this will be an overwhelming circumstance for database server to validate the lecture room, course, time allocated for each student, a huge number of solicitations of thousands of students needs to be taken care of by the database server. For attendance purpose at the lecturer rooms, the concerned records are queried from the database server to the installed middleware at the start of each lecturer to the assigned lecturer room. The attendance is taken through RFID reader and saved locally in the raspberry Pi middleware until the predefined term for authorization to enter the lecture room is finished. Then, at that point the middleware sends all the records to the database server. The nearby transitory stockpiling of the records and query by middleware decline incessant correspondence with database server and thus expands the productivity of the framework.

3.6 Algorithms

The algorithms designed for physical security at main entrances SECURITY and for ATTENDANCE at the door of each lecturer room, completely presented with comments to each progression, see Figure 3 & 4 respectively.

4. Results and discussions

ALGORITHM 1: AUTHENTICATING SYSTEM

Input: RFID reader reads the RFID card and pass it to the Raspberry Pi, at the Main Entrance(s)
Output: Person Authenticated enters the institution by Green or Red LED.

```
readId ← 0;
waitCount ← 1;
// One time loading of Ids at time of system initiation to the local repository
preloadedIds ←ReadDatabaseRecord();
// Motion detection
if (MotionDetected()) then
    // Waiting for reading the Id from the RFID card (tag) by RFID reader assigned to a person
    while (!RfidDetected()) do
        // One second wait
        waitCount++;
        if (waitCount == 3) then
            response ← FALSE
            waitCount ← 1
            // End of the program execution
            end
        end
    end
    // Reading Id (tag) from the RFID card
    readId = ReadID();
    // Loading Id and returning index
    FoundNumberIndex ←BinarySearch(preloadedIds[],readId);
    if (FoundNumberIndex ≤ 0) then
        / / Response generated by middleware (raspberry Pi) is passed to the Arduino for
        turning GREEN LED on
        response ← TRUE;
    else
        / / Response generated by middleware (raspberry Pi) is passed to the Arduino for
        turning RED LED on
        response ← FALSE;
    end
end
// Do nothing; wait for RFID card to read
```

Fig 3: Authentication System Algorithm at KsTU main gate.

ALGORITHM 2: CHECK ATTENDANCE

Input: RFID reader reads the RFID card and pass it to the Raspberry Pi, at the Class Room Door

Output: Records attendance after validation of Subject, Lecture Room, Time slot in time table

```
readId ← 0;
waitCount ← 1;
// E.g. Lecture room, Lab etc
roomId ←roomName;
// Days of the week E.g. Monday, Tuesday etc
dayId ←dayName;
// System time
timeId ←sysTime;
// Counter minutes from the beginning
minutId ←Counter;
if (timeId == 0) then
    hourId ←hour; //Hourcountdown
    // Fetching and validating students who has class in the specified Lecture room on the current
    day and slot to the middleware (Raspberry Pi)
    loadStdIds[] ←ReadDatabaseRecord(hourId,roomId,dayId);
else
    // Detecting RFID card
    if (RfidDetected()) then
        // Reading Id from the RFID card and pass on to the middleware for validation
        readId ←ReadID();
        // Looking for id and returning the index
        FoundNumberIndex ←BinarySearcH(loadStdIds[ ],readId);
        if (FoundNumberIndex ≤ 0) then
            // Middleware pass on the negative response to RFID reader (arduino) for turning
            RED LED on
            response ← FALSE;
        else
            indexOfRecord ←FoundNumberIndex;
            // Middleware pass on the positive response to RFID reader (arduino) for turning
            GREEN LED on
            response ← TRUE;
            while (!RfidDetected()) do
                waitCount++; // One second wait
                if (waitCount == 3) then
                    response ← FALSE
                    waitCount ← 1
                    end // End of the program execution
                end


        end
        // After 10 minutes the system will not read RFID cards (the time is depends on the
        rules of university or organization)
        if (minutId == 10 ) then
            for i ← 0to n − 1 do
                // Insert present student Id to the database
                databaseInsert(presentStdId[i]);
            end
            for j ← 0to n − 1 do
                // Insert absent student Id to the database
                databaseInsert(absentStdId[j]);
            end
            else
                // Recording the attendance locally
                presentStdId[indexOfRecord] ←absentStdId[indexOfRecord];
                // Deleting record from pre-loaded array locally
                absentStdId[indexOfRecord] ← null
                Sort(presentStdId);
                Sort(absentStdId);
            end
    end
```

Fig 4: Algorithm for Checking Attendance.

4.1 Hypothetical Analysis

The system is breaking down hypothetically utilizing estimation of every assessment end. The effectiveness of system is hypothetically estimated by two parameters for example the system deployment and conformity generally relies upon the expense on the grounds that KstU as a world class University needs assurance on security, so practical system might be more appropriate for use. The other significant factor to be considered is time proficiency. Both the assessed cost and assessed time are momentarily portrayed below.

4.2 Estimated Cost

The expense of arrangement of the proposed system is measured for two distinct positions for main gate entrance(s) and lecture rooms. The estimated cost in Ghana cedis and US dollars are summed up in Table 2.

The complete expenses rely upon the reach and sort of the gadgets utilized and is registered by the current costs in the market as at August 2021. A portion of the gadgets has one time cost, for example local server or client PC. The gadgets like RFID can influence the general deployment cost. The absolute expense per lecture room ranges between $1000 to $1500 roughly as displayed in table 2.

		Estimated Costs	
Device	**Device Type Or Range**	**GH₵**	**US$**
Raspberry Pi	Raspberry Pi	640	109
RFID	13Mhz (10cm-15cm) 856Mhz (3m)	600 300	100 50
Arduino	Arduino	60 440	10 73
Motion Sensor	Motion Sensor	400	70
Wires, Resistors, LED etc.	General	120	20
40 RFID tags	General	36	6
Total Cost Per Class	Short Range	460	76

Room	Long Range	1086	180
Server PC	-	3018.14	600

Table 2: Estimated Cost For Short And Long Range Devices.

4.3 Assessed Time

The system verifies individual devouring around three seconds, which is typical human walk speed. So approximately best-case scenario the system can verify around 20 people what's more, subsequently more than 1200 people in a single hour at the main gate.

The time relies upon human rather the system, on the off chance that somebody covers 2 feet distance quicker than 1 second, the system takes that measure of time to validate or record the attendance, furthermore, make the verification process smoother. Essentially during lectures, the time taken relies upon the speed of the student to walk to the lecture room. On estimating lecture room with student of 46 won't require over 2 minutes to record the attendance. Additionally, the server won't be overpowering with user demand due local attendance storage. For instance: if there are active lectures rooms to be used by 300 hundred students, it means user request to the Server will not be less than 300.

5. Conclusion

A positive learning experience involves every aspect of creating a safe learning environment. Physical space for learning is very important for staffs and students. A learning environment that is free of treat, psychological harm and violence allows students and lecturers to express their views honestly. Giving a secured learning climate to Students, staff (faculty and administrators), supports the positive conduct that raises scholarly splendor. This research proposed a system for actual security for Kumasi Technical University which would be utilized for attendance of the students. Two algorithms have been intended for productive usage of RFID innovation for this reason. The system has been dissected theoretically in terms of cost which is moderate for any educational institution and likewise examined as far as time utilization to confirm individual at main entrance, during attendance

which isn't more than time taken by regularly human walk. . The implementation of this study will provide serene ground which will promote teaching and learning environment to demonstrate a comfort learning environment without controversy and conflict, this will promote classroom participation and above all promote Kumasi Technical University as a welcoming environment where learners feels physically, emotionally and socially comfortable.

6. Conflict of interest

The authors declare that they have no conflict of interest.

7. References

[1] Lamport L, Password authentication with insecure communication. Commun. ACM 1981,24, 770–772.

[2] MONTANO B, Biometric validation method and biometric terminal. Aug 2015, [online] Available: https://www.mysciencework.com/patent/show/biometric-validation-method-biometric-terminal-EP2911106A1 . Accessed on: 17/9/2021

[3] Swanson J, Git Ransom Campaign Incident Report-Atlassian Bitbucket, GitHub, GitLab. The GitHub Blog, September 17, 2019. https://github.blog/2019-05-14-git-ransom-campaign-incident-report/.

[4] Thomas K, & Angelika M, New Research: How Effective Is Basic Account Hygiene at Preventing Hijacking. Google Online Security Blog, May 17, 2019. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html.

[5] Bissada A, and Olmsted A, Mobile multi-factor authentication, *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2017.

[6] Insan M, Sukarno P, and Yasirandi R, Multi-factor authentication using a smart card and fingerprint (case study: Parking gate), *Indonesia Journal on Computing (Indo-JC)*, vol. 11, no. 4, pp. 55-66, Nov. 2019, [online] Available: https://doi.org/10.21108/INDOJC.2019.4.2.309.

[7] O'Neill M, Insecurity by Design: Todays IoT Device Security Problem, *Elsevier Journal on Engineering*, vol. 2, no. 1, pp. 48-49, March 2016.

[8] Hicks M J, Yates, Jago W H, Phillips A W & Togo D F, Cost and Performance Analysis of Physical Security Systems, *ADPA/NSIA 13 Annual Security Technology Symposium & Exhibition Government-Industry Exchange*, 1997-June-9-12.

[9] Reid R N, Facility manager's guide to security: Protecting your assets the Fairmont Press, Inc., 2005.

[10] Fennelly L, Effective physical security. Butterworth-Heinemann, 5th edition (November 28, 2016)

[11] https://www.ifsecglobal.com/cyber-security/4-drawbacks-of-biometric-authentication/ Accessed on: 18th August, 2021.

[12] McKenna S, & Butler M. –International Journal of Biometrics, 2016 - inderscienceonline.com

[13] Gottfried M A, *Evaluating the Relationship Between Student Attendance and Achievement in Urban Elementary and Middle Schools: An Instrumental Variables Approach* American Educational Research Journal, :2010.

[14] Manavalan EM, & Jayakrishna K, A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements Computers & Industrial Engineering, Volume 127, :2019, Pages 925-953, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2018.11.030.

[15] Ignat C, International Scientific Conference Strategies XXI; Bucharest Vol. 2, : 216-224. Bucharest: Carol I National Defence University. (2016)

[16] D Ponnimbaduge Perera D, Jayakody D N K , Sharma, S K Chatzinotas S, & Li J Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advances and Future Challenges, in *IEEE Communications Surveys & Tutorials*, vol 20, no 1, pp 264-302, Firstquarter : 2018, doi: 10 1109/COMST 2017 2783901