**Internet of Things (IoT)** là một công nghệ mới nổi kết nối nhiều loại thiết bị, bao gồm điện thoại thông minh, thiết bị gia dụng, cảm biến và các thiết bị mạng khác. Công nghệ mới này có thể được áp dụng trong nhiều lĩnh vực ứng dụng, chẳng hạn như nhà thông minh (ví dụ: bảo mật, sưởi ấm và kiểm soát ánh sáng), thành phố thông minh, chăm sóc sức khỏe (ví dụ: từ xa theo dõi bệnh nhân) và sản xuất thông minh (ví dụ: từ xa giám sát và kiểm soát hệ thống sản xuất).

Các mạng (5G) hiện đang được phát triển đang hướng tới mục tiêu cung cấp cao tốc độ (1 Gbps), công suất thấp và độ trễ thấp (1 ms trở xuống). Do đó công nghệ 5G sẽ đẩy nhanh việc triển khai nhiều Các ứng dụng IoT, đòi hỏi sự phổ biến hơn, tính di động cao hơn, hiệu suất và tốc độ tốt hơn, và thời gian đáp ứng nhanh hơn.

Mạng cảm biến không dây (WSN) bao gồm một số lượng lớn các nút cảm biến nhỏ, không bị hạn chế về tài nguyên, triển khai trong một lĩnh vực quan tâm để theo dõi và thu thập vật lý hoặc các điều kiện môi trường, chẳng hạn như ánh sáng, nhiệt độ, áp suất, chuyển động, âm thanh hoặc chất ô nhiễm. WSN đóng vai trò quan trọng vai trò trong IoT bằng cách hỗ trợ cảm biến và thu thập thông tin môi trường. Do đó, để cung cấp thành công IoT các ứng dụng, sự tích hợp của mạng 5G và WSN là cần thiết.

Tuy nhiên, bất chấp tiềm năng của sự tích hợp này, nó cũng phơi bày chúng ta hơn nữa đối với các mối đe dọa về bảo mật.

Do đó, bảo mật và quyền riêng tư là rất quan trọng để bảo vệ IoT các ứng dụng từ các cuộc tấn công như vậy. Hơn nữa, sự không đồng nhất của các mạng có thể có một ảnh hưởng đáng kể đến bảo mật các ứng dụng IoT , trong đó hạn chế về tài nguyên các nút cảm biến phải mở một giao tiếp an toàn với nhiều hơn thiết bị mạnh mẽ.

Ví dụ, trong một ngôi nhà thông minh, ngôi nhà các nút cảm biến giao tiếp với điện thoại thông minh người dùng. Dành cho liên lạc an toàn giữa bất kỳ bên nào và để cung cấp mức độ bảo mật tương đương để liên lạc giữa các thiết bị khác nhau, thuật toán mã hóa tối ưu là rất cần thiết.

Hơn nữa, các thiết bị IoT yêu cầu tốc độ cao và hiệu quả an ninh nhẹ. Trong IoT, chỉ những người dùng hợp pháp mới có thể truy cập các thiết bị IoT xác thực (nghĩa là, một cổng hoặc nút cảm biến) và một phiên xác thực nên được thiết lập giữa người dùng và thiết bị IoT để truyền dữ liệu an toàn. Do đó, xác thực lẫn nhau với thỏa thuận chính là một yêu cầu quan trọng đối với IoT. Bởi vì IoT mang dữ liệu có thể chứa thông tin riêng tư cá nhân (nghĩa là, danh tính và vị trí) và bất kỳ ai cũng có thể truy cập thiết bị khác của người dùng, bất kỳ rò rỉ thông tin có thể ảnh hưởng đến quyền riêng tư của người dùng.

Trong 5G WSN được phân cấp cho IoT, ẩn danh là một khía cạnh bảo mật quan trọng, bởi vì nó bảo vệ quyền riêng tư của cả người dùng và các thiết bị IoT như các nút cảm biến. Ẩn danh thông thường đề cập đến trạng thái trong đó một cá nhân cá nhân hoặc thông tin nhận dạng cá nhân không được biết công khai. Khả năng không liên kết của hai hoặc nhiều mục quan tâm, từ một quan điểm của kẻ tấn công, có nghĩa là trong hệ thống, Kẻ tấn công không thể xác định liệu các mục này có liên quan. Pfitzmann và Hansen chỉ ra rằng tính không liên kết là đủ điều kiện ẩn danh, nhưng không phải là điều kiện cần thiết. Tuy nhiên, để hoàn toàn ẩn danh, hầu hết người dùng đều muốn ẩn danh mạnh mẽ, đòi hỏi không liên kết. Vì vậy, để bảo vệ quyền riêng tư của người dùng, cả hai ẩn danh và không liên kết nên được xem xét.

**A. CÔNG VIỆC LIÊN QUAN**

Năm 2006, Wong và cộng sự. đề xuất một lược đồ xác thực người dùng nhẹ [8] cho các WSN dựa trên XOR và hàm băm hoạt động. Tuy nhiên, vào năm 2009, Das đã cho thấy kế hoạch này không thể chịu được một cuộc tấn công xác minh bị đánh cắp và một cuộc tấn công nơi nhiều người dùng đã đăng nhập với cùng một ID và do đó, đề xuất một sơ đồ xác thực người dùng dựa trên hai yếu tố để giải quyết những vấn đề này. Trong sơ đồ của mình, một mật khẩu và thông minh Thẻ được sử dụng như hai yếu tố để xác thực người dùng. Tuy nhiên, vào năm 2010, một số nhà nghiên cứu - đã chỉ ra các vấn đề bảo mật trong sơ đồ Das, và đề xuất cải tiến vượt qua. Sau đó, Das et al. vào năm 2012 và Xue et al. Năm 2013 trình bày xác thực người dùng và khóa các lược đồ thỏa thuận cho các WSN dựa trên việc sử dụng thông minh thẻ.

Gần đây, vào năm 2014, Turkanovic et al. đề xuất một người dùng kế hoạch và thỏa thuận chính cho không đồng nhất các WSN đặc biệt, dựa trên IoT. Đề án của họ là nhẹ vì nó chỉ sử dụng các thao tác đơn giản, chẳng hạn như Hàm XOR và hàm băm. Thông qua IoT, một người dùng ngẫu nhiên có thể kết nối trực tiếp với một nút cảm biến từ WSN và đàm phán khóa phiên với nó mà không kết nối với nút cổng. Thật không may, kế hoạch này sau đó đã được chứng minh là dễ bị tấn công bởi nhiều cuộc tấn công, bởi Chang et al, Farashet al, Amin và Biswas và Tai et al .

Năm 2016, Chang et al chỉ ra rằng Turkanovic và cộng sự lược đồ dễ bị tấn công mạo danh với nút chụp, một cuộc tấn công thẻ thông minh bị đánh cắp, giả mạo nút cảm biến tấn công và tấn công xác minh bị đánh cắp, cũng như không đảm bảo bí mật lạc hậu. Chang et al. đề xuất một cách linh hoạt giao thức xác thực bằng thẻ thông minh cho các WSN hoạt động ở hai chế độ: sơ đồ xác thực nhẹ, như một sự cải tiến so với Turkanovic et al. sơ đồ, và ắc một giao thức nâng cao dựa trên mật mã đường cong elliptic (ECC), cung cấp bí mật hoàn hảo về phía trước. Đồng thời, Farash et al. xác định rằng Turkanovic hunget al. lược đồ không thể chống lại một cuộc tấn công thẻ thông minh bị đánh cắp và một cuộc tấn công trung gian và nó không cung cấp, không thể kiểm soát và bí mật tiến / lùi. Dựa trên phân tích của họ, họ đã đề xuất một xác thực người dùng được cải thiện và lược đồ thỏa thuận chính cho các WSN không đồng nhất. Tuy nhiên, Amin et al. thấy rằng chương trình Farash et al. chịu được thông tin tạm thời cụ thể theo phiên tấn công, một cuộc tấn công đoán mật khẩu ngoại tuyến bằng cách sử dụng một đánh cắp tấn công thẻ thông minh, tấn công phát hành thẻ thông minh mới và tấn công mạo danh người dùng. Hơn nữa, nó không bảo tồn ẩn danh người dùng và bí mật của khóa bí mật của nút cổng. Amin và cộng sự. sau đó trình bày một giao thức trao đổi khóa xác thực ba yếu tố ẩn danh đối với WSN, trong đó mật khẩu, thẻ thông minh và sinh trắc học được sử dụng như ba yếu tố.

Năm 2016, Amin và Biswas đã chứng minh rằng Turkanovicetiên Chương trình al. không ngăn chặn mật khẩu nhận dạng ngoại tuyến đoán tấn công, tấn công trộm thẻ thông minh, tấn công mạo danh người dùng và tấn công mạo danh nút cảm biến, cũng như cung cấp một giai đoạn xác thực không hiệu quả. Như một Giải pháp, họ đề xuất một sơ đồ nhẹ an toàn cho người dùng xác thực và thỏa thuận quan trọng trong đa cổng dựa WSN.

Gần đây nhất, năm 2017, Tai et al. cũng cho thấy rằng Sơ đồ Turkanovic và cộng sự không đảm bảo tính ẩn danh của người dùng, và rằng một khóa phiên được thiết lập trong sơ đồ có thể là rò rỉ bằng cách sử dụng các nút cảm biến bị xâm nhập. Để khắc phục những lỗ hổng bảo mật, họ đề xuất cải tiến cho Turkanovicet al. Đề án. Họ tuyên bố rằng chương trình của họ đảm bảo người dùng ẩn danh và xác thực lẫn nhau giữa tất cả các bên. Tuy nhiên, chúng tôi đã phát hiện ra rằng chương trình Tai et al. cung cấp xác thực lẫn nhau và ẩn danh nút cảm biến và hơn nữa, nó dễ bị nút cảm biến tấn công giả mạo với việc bắt nút cảm biến, tấn công đặc quyền và thông tin tạm thời theo phiên cụ thể tấn công. Chúng tôi cũng tìm thấy những điểm yếu bảo mật bổ sung trong Đề án, cụ thể là, dễ bị đánh cắp thẻ thông minh và các cuộc tấn công đoán mật khẩu ngoại tuyến và không đảm bảo ẩn danh người dùng.

**B. ĐÓNG GÓP**

Như thể hiện trong phần về các công việc liên quan, các nghiên cứu hiện có về xác thực người dùng và thỏa thuận chính cho WSN không thành công Đáp ứng các tính năng bảo mật mong muốn. Đặc biệt, hầu hết đề án đề xuất không cung cấp ẩn danh mạnh mẽ, được đề cập để không liên kết. Ngoài ra, họ tập trung chủ yếu vào các WSN, có nghĩa là kiến ​​trúc mạng của họ không phù hợp với Các WSN tích hợp 5G cho IoT.

• Chúng tôi phân tích bảo mật của Tai et al., Gần đây nhất xác thực người dùng và lược đồ thỏa thuận chính cho các WSN không đồng nhất về quảng cáo không đồng nhất. Chúng tôi cho thấy rằng sơ đồ của họ dễ bị tấn công bao gồm đánh cắp thẻ thông minh, đoán mật khẩu ngoại tuyến, cảm biến giả mạo nút, đặc quyền nội bộ và phiên cụ thể tấn công thông tin tạm thời. Chúng tôi cũng cho thấy rằng Tai et al. Lược đồ không bảo tồn nút người dùng và cảm biến ẩn danh, xác thực lẫn nhau và bí mật của khóa bí mật của nút cổng.

• Chúng tôi thiết kế kiến ​​trúc mạng phù hợp với các WSN 5Gintegrated cho IoT. Theo mạng mới

kiến trúc, chúng tôi đề xuất một xác thực hai yếu tố an toàn và sơ đồ thỏa thuận chính khắc phục điểm yếu bảo mật nói trên và bảo tồn tất cảc ác tính năng bảo mật của chương trình Tai et al. Hơn thế nữa, kế hoạch đề xuất của chúng tôi chịu được tất cả các cuộc tấn công đã biết và đảm bảo tính không liên kết và do đó, ẩn danh mạnh mẽ.

• Sử dụng đánh giá bảo mật, chúng tôi cho thấy rằng đề xuất của chúng tôi Đề án có thể chống lại nhiều cuộc tấn công, bao gồm cả những cuộc tấn công sẽ thỏa hiệp chương trình Tai et al. Ngoài ra, chúng tôi so sánh các tính năng bảo mật của chương trình đề xuất của chúng tôi với những đề án liên quan khác.

• Thông qua đánh giá hiệu suất, chúng tôi so sánh thực hiện kế hoạch đề xuất của chúng tôi với các liên quan khác đề án về chi phí tính toán, chi phí truyền thông và chi phí lưu trữ.

**C. TỔ CHỨC GIẤY**

Phần 2 đánh giá ngắn gọn sơ đồ Tai et al., Sau đó chúng tôi thảo luận về các điểm yếu bảo mật của nó trong Phần 3. Mục 4 giải quyết các xác thực được đề xuất và thỏa thuận chính sơ đồ với khả năng không liên kết, dựa trên thiết kế mạng mới. Đánh giá bảo mật của chương trình đề xuất được thảo luận trong Phần 5. Mục 6 trình bày so sánh hiệu suất với các đề án liên quan khác. Cuối cùng, chúng tôi kết luận bài báo trong phần 7.

**VII. PHẦN KẾT LUẬN**

Trong bài báo này, chúng tôi đã xem xét sơ đồ Tai et al. Và chứng minh rằng nó dễ bị tấn công bằng thẻ thông minh bị đánh cắp, tấn công đoán mật khẩu ngoại tuyến, tấn công giả mạo nút cảm biến, tấn công từ nội bộ và tấn công thông tin tạm thời theo phiên cụ thể.

Chúng tôi tiếp tục chỉ ra rằng Tai et al. lược đồ không bảo vệ ẩn danh nút người dùng và cảm biến, xác thực lẫn nhau và bí mật của khóa bí mật của nút cổng.. Dựa vào cái này kiến trúc mạng, chúng tôi đã đề xuất một yếu tố an toàn hai yếu tố xác thực và chương trình thỏa thuận quan trọng với khả năng không liên kết. Chúng tôi đã đánh giá tính bảo mật của chương trình đề xuất và so sánh nó với các đề án liên quan khác. Kết quả cho thấy kế hoạch đề xuất là an toàn chống lại nhiều người biết các cuộc tấn công và nó đáp ứng tất cả các tính năng bảo mật, bao gồm không liên kết, cần thiết để xác thực người dùng an toàn và thỏa thuận chính.

Chúng tôi cũng đã đánh giá hiệu suất của đề án đề xuất về chi phí tính toán, chi phí truyền thông và chi phí lưu trữ, sau đó chúng tôi so sánh với những đề án khác có liên quan. Các kết quả đánh giá về bảo mật và hiệu suất cho thấy chương trình của chúng tôi cung cấp tốt hơn an toàn mà không có hiệu suất khác biệt đáng kể so với khác đề án, và kết quả thực hiện được dự kiến ​​sẽ cải thiện bởi vì cổng hoạt động tốt hơn nút cảm biến trong Các WSN tích hợp 5G cho IoT.

Trong công việc tương lai, chúng tôi sẽ đo lường hiệu suất của lược đồ được đề xuất bằng cách triển khai và thực hiện các thử nghiệm sử dụng các thiết bị thực tế trên các WSN tích hợp 5G cho IoT (ví dụ: điện thoại thông minh và thiết bị cảm biến) và, sẽ cải thiện đề án dựa trên kết quả thí nghiệm.